#### Lecture 5: Principles of Security

CS 181S

September 19, 2018

### Last Time

- 1. Functional requirements
- 2. Threat analysis
- 3. Harm analysis
- 4. Security goals
- 5. Feasibility analysis
- 6. Security requirements



#### Example: ELEANOR'S PLACE

- New restaurant in Claremont
- You are contracted to build a system for online reservations
- What are the functionality requirements for this reservation system?
- What is the threat model?
- What confidentiality, integrity, and availability harms does Eleanor's Place face?
- What security goals should it have?
- Are they feasible? How could these be refined to security requirements?
- What countermeasures could be employed to implement security requirements?

#### Countermeasures

Introduction to Security1WedSep 5Security Policles [sides] [pdf][Bihop, Ch. 1.1.1.3]2MonSep 10Vulnerabilities [sides] [pdf](Notes] [Review Exercises]3MonSep 12Threat Worde's [sides] [pdf]Notes] [Review Exercises]3MonSep 13Security PrinciplesA1 DUE4MonSep 24Security Principles[Schneider, Ch. 1], [Saltzer-Schneider]4MonSep 25Security Principles[Schneider, Ch. 1], [Saltzer-Schneider]4MonSep 26Symmetric CryptoMo DUE5MonOct 1Public-Key CryptographyMo DUE5MonOct 3Secure ChannelsM1 DUE6MonOct 1Public-Key CryptographyMo DUE6MonOct 1Protocol DesignM2 DUE7WedOct 17Human Authentication[Schneider, Ch. 5]T2 DUE8MonOct 2Fall Review SocialM2 DUE9MedOct 31CertificatesA2 DUE9MonNov 5DAC[Schneider, Ch. 7.3]9MonNov 5DAC[Schneider, Ch. 7.3]10MonNov 5DAC[Schneider, Ch. 7.3]11MedNov 10Information Flow[notes]12MonNov 12If AnalyzianM3 DUE13MedNov 13IFC (cont'd)[notes]14MonNov 26LogsM3 D	Week	Day	Date	Торіс	Reading	Due
Mon         Sep 10         Vulnerabilities [sides] [pdf]         [Notes] [Review Exercises]           Wed         Sep 12         Threat Models [sides] [pdf]         T1 DUE           Mon         Sep 17         Beyond Threats         A1 DUE           Wed         Sep 19         Security Principles         A1 DUE           Wed         Sep 24         Security Principles         [Schneider, Ch 1], [Saltzer-Schroeder]           Wed         Sep 26         Symmetric Cryptography         M0 DUE           Secure Channels         M1 DUE         M0 Oct 8         Protocol Design           Wed         Oct 3         Secure Channels         M1 DUE           Mon         Oct 8         Protocol Design         A2 DUE           Wed         Oct 10         Key Management         A2 DUE           Wed         Oct 17         Human Authentication         [Schneider, Ch. 5]         T2 DUE           Mon         Oct 22         Fal Reces, No Class         M2 DUE           Wed         Oct 39         Tokens         M2 DUE           Mon         Oct 29         Tokens         M2 DUE           Mon         Oct 29         Tokens         M3 DUE           Mon         Nov 12         M2         [Bichop, Ch. 7.3]				Introduction	to Security	
Wed         Sep 12         Threat Models [slides] [pd]         T1 DUE           3         Mon         Sep 17         Beyond Threats         A1 DUE           4         Mon         Sep 19         Security Principles         A1 DUE           4         Mon         Sep 24         Security Principles         A1 DUE           4         Mon         Sep 24         Security Principles         Mon           4         Mon         Sep 24         Security Principles         Mon           5         Mon         Oct 1         Public-Key Cryptography         Mon DUE           5         Mon         Oct 3         Secure Channels         M1 DUE           6         Mon         Oct 3         Secure Channels         M1 DUE           7         Mon         Oct 15         Applied Cryptography         T2 DUE           7         Mon         Oct 15         Applied Cryptography         M2 DUE           7         Mon         Oct 17         Human Authentication         [Schneider, Ch. 5]         T2 DUE           8         Mon         Oct 22         Fall Recess, No Class         M2 DUE         M2 DUE           9         Mon         Oct 29         Tokens         M2 DUE         M3	1	Wed	Sep 5	Security Policies [slides] [pdf]	[Bishop, Ch. 1.1-1.3]	
Mon       Sep 17       Beyond Threats       A1 DUE         Wed       Sep 19       Security Principles       A1 DUE         4       Mon       Sep 24       Security Principles       [Schneider, Ch. 1], [Sattzer-Schroeder]         Wed       Sep 25       Symmetric Cryptography       Mo       M0 DUE         5       Mon       Oct 1       Public-Key Cryptography       M1 DUE         6       Oct 3       Secure Channels       M1 DUE         7       Mon       Oct 10       Key Management       A2 DUE         7       Mon       Oct 15       Applied Cryptography       To UE         Wed       Oct 17       Human Authentication       [Schneider, Ch. 5]       T2 DUE         80       Mon       Oct 22       Fall Recess, No Class       M2 DUE         91       Med       Oct 31       Certificates       A3 DUE         92       Mon       Nor 5       DAC       [Schneider, Ch. 7.3]       M3 DUE         93       Mon       Nor 5       DAC       [Schneider, Ch. 7.3]       M2 DUE         94       Nor 10       Cet216       Capabilities       [Schneider, Ch. 7.3]       Bishop, Ch. 14.2]       T3 DUE         94       Nor 12       MLS <td rowspan="2">2</td> <td>Mon</td> <td>Sep 10</td> <td>Vulnerabilities [slides] [pdf]</td> <td>[Notes] [Review Exercises]</td> <td></td>	2	Mon	Sep 10	Vulnerabilities [slides] [pdf]	[Notes] [Review Exercises]	
WedSep 19Security PrinciplesIschneider, Ch. 1), [Saltzer-Schneder]4MonSep 24Security Principles[Schneider, Ch. 1), [Saltzer-Schneder]5WedSep 25Symmetric CryptographyMO DUE5MonOct 1Public-Key CryptographyMI DUE6MonOct 3Secure ChannelsMI DUE6MonOct 8Protocol DesignA2 DUE7MonOct 15Applied CryptographyA2 DUE7MonOct 15Applied CryptographyA2 DUE7MonOct 15Applied CryptographyMI DUE7MonOct 12Foll Recess, No ClossM2 DUE8MonOct 22Foll Recess, No ClossM2 DUE9MonOct 22Foll Recess, No ClossM2 DUE9MonOct 22Foll Recess, No ClossM2 DUE9MonNov 5DACSchneider, Ch. 7.3]M3 DUE10MonNov 5DACSchneider, Ch. 7.3]M3 DUE11MonNov 12MLSBishop, Ch. 14.2]T3 DUE12MonNov 12Thonksgiving, No ClassM3 DUE13MonNov 25LogsM3 DUE14MonNov 26LogsTablied Scands]M3 DUE14MonNov 26LogsTablied Scands]M3 DUE15MonNov 25LogsTablied Scands]M3 DUE16MonNov 26Logs <td>Wed</td> <td>Sep 12</td> <td>Threat Models [slides] [pdf]</td> <td></td> <td>T1 DUE</td>		Wed	Sep 12	Threat Models [slides] [pdf]		T1 DUE
Mon       Sep 24       Security Principles       [Schneider, Ch. 1], [Saltzer-Schroeder]         Wed       Sep 26       Symmetric Crypto       Mo DUE         Secure       Man       Oct 1       Public-Key Cryptography       Mi DUE         Wed       Oct 3       Secure Channels       Mi DUE         Mon       Oct 8       Protocol Design       A2 DUE         Wed       Oct 10       Key Management       A2 DUE         Wed       Oct 17       Human Authentication       [Schneider, Ch. 5]       T2 DUE         Mon       Oct 22       Fall Recess, No Class       M2 DUE         Wed       Oct 31       Cettificates       M3 DUE         Mon       Oct 32       Fall Recess, No Class       M2 DUE         Wed       Oct 31       Cettificates       M3 DUE         Mon       Oct 32       Fall Recess, No Class       M2 DUE         Wed       Oct 31       Cettificates       M3 DUE         Mon       Nov 7       Capabilities       [Schneider, Ch. 7.3]       M3 DUE         Mon       Nov 7       Capabilities       [Schneider, Ch. 7.3]       M3 DUE         Mon       Nov 12       MLS       [Bishop, Ch. 5-6.2]       M3 DUE         Wed	3	Mon	Sep 17	Beyond Threats		
Cryptography         Mo         M		Wed	Sep 19	Security Principles		A1 DUE
WedSep 26Symmetric CryptoM0 DUE5MonOct 1Public-Key CryptographyM1 DUE6MonOct 3Secure ChannelsM1 DUE6MonOct 8Protocol DesignA2 DUE7MonOct 15Applied CryptographyA2 DUE7MonOct 15Applied CryptographyAuthenticationSecure CryptographyWedOct 17Human Authentication[Schneider, Ch. 5]T 2 DUE8MonOct 22Fall Reces, No ClassM2 DUE9MonOct 24PasswordsM2 DUE9MonOct 31CertificatesA3 DUE9MonNov 5DAC[Schneider, Ch. 7.3]M3 DUE10MonNov 5DAC[Schneider, Ch. 7.3]Bishop, Ch. 14.2]T3 DUE11MonNov 12MLS[Bishop, Ch. 5-6.2]T12MonNov 19IFC (cont'd)[notes]M3 DUE12MonNov 26LogsTT13MonNov 28BlockchainsT4 DUE14MonDec 3Network Security[notes]T4 DUE15MonDec 10Privacy[notes]M4 DUE	4	Mon	Sep 24	Security Principles	[Schneider, Ch. 1], [Saltzer-Schroeder]	
Mon         Oct 1         Public-Key Cryptography           Wed         Oct 3         Secure Channels         M1 DUE           6         Mon         Oct 3         Secure Channels         M1 DUE           6         Mon         Oct 10         Key Management         A2 DUE           7         Mon         Oct 13         Applied Cryptography         A2 DUE           7         Mon         Oct 13         Applied Cryptography         A2 DUE           7         Mon         Oct 14         Applied Cryptography         A2 DUE           7         Mon         Oct 15         Applied Cryptography         T2 DUE           8         Mon         Oct 14         Puson Authentication         [Schneider, Ch. 5]         T2 DUE           8         Mon         Oct 22         Fall Recess, No Class         M2 DUE         M2 DUE           9         Mon         Oct 23         Certificates         A3 DUE         M2 DUE           9         Mon         Oct 31         Certificates         [Schneider, Ch. 7.3]         M3 DUE           10         Mon         Nov 5         DAC         [Schneider, Ch. 7.3]         [Bishop, Ch. 14.2]         T3 DUE           11         Mon         Nov 14				Cryptog	graphy	
WedOct 3Secure ChannelsM1 DUE6MonOct 8Protocol DesignA2 DUEWedOct 10Key ManagementA2 DUE7MonOct 15Applied CryptographyT2 DUEAuthentication[Schneider, Ch. 5]T2 DUE8MonOct 22Fail Recess, No ClassM2 DUE9MonOct 24PasswordsM2 DUE9MonOct 29TokensM2 DUE9MonOct 29TokensM2 DUE9MonNov 5DAC[Schneider, Ch. 7.3]T3 DUE10MonNov 5DAC[Schneider, Ch. 7.3]Bishop, Ch. 14.2]T3 DUE11MonNov 12MLS[Bishop, Ch. 5-6.2]M3 DUE12MonNov 19IFC (contd)Inotes]M3 DUE12MonNov 19IFC (contd)Inotes]M3 DUE12MonNov 28BlockchainsT4 DUE13MonNov 28BlockchainsT4 DUE14MonDec 3Network Security[notes]M4 DUE15MonDec 5Web Security[notes]M4 DUE15MonDec 10Privacy[notes]M4 DUE		Wed	Sep 26	Symmetric Crypto		M0 DUE
6MonOct 8Protocol DesignWedOct 10Key ManagementA2 DUE7MonOct 15Applied CryptographyFurtherticationSchneider, Ch. 5)T2 DUEWedOct 17Human Authentication[Schneider, Ch. 5)T2 DUE8MonOct 22 <i>Fall Recess, No Class</i> M2 DUE9MonOct 29TokensM2 DUE9MonOct 29TokensA3 DUE9MonNov 5DAC[Schneider, Ch. 7.3]T3 DUE10MonNov 5DAC[Schneider, Ch. 7.3]T3 DUE11MonNov 12MLS[Bishop, Ch. 5-6.2]T3 DUE12MonNov 13IFC (cont'd)[notes]M3 DUE12MonNov 19IFC (cont'd)[notes]T4 DUE13MonNov26LogsT4 DUE14MonDec 3Network Security[notes]T4 DUE15MonDec 3Network Security[notes]M4 DUE15MonDec 3Network Security[notes]M4 DUE	5	Mon	Oct 1	Public-Key Cryptography		
WedOct 10Key ManagementA2 DUE7MonOct 15Applied CryptographyKuthenticationWedOct 17Human Authentication[Schneider, Ch. 5]T2 DUE8MonOct 22Fall Recess, No ClassM2 DUE9MonOct 29TokensM2 DUE9MonOct 31CertificatesA3 DUE10MonNov 5DAC[Schneider, Ch. 7.3]T3 DUE11MonNov 7Capabilities[Schneider, Ch. 7.3]T3 DUE12MonNov 12MLS[Bishop, Ch. 7.3]Bishop, Ch. 14.2]T3 DUE12MonNov 12MLS[Bishop, Ch. 5-6.2]T13MonNov 19IFC (cont'd)[notes]M3 DUE14MonNov 26LogsT4 DUE15MonNov 26LogsT4 DUE14MonDec 3Network Security[notes]T4 DUE15MonDec 5Web Security[notes]M4 DUE15MonDec 5Web Security[notes]M4 DUE		Wed	Oct 3	Secure Channels		M1 DUE
Mon         Oct 15         Applied Cryptography           Authentication           Wed         Oct 17         Human Authentication         [Schneider, Ch. 5]         T2 DUE           Mon         Oct 22         Fall Recess, No Class         T2 DUE           Mon         Oct 24         Passwords         M2 DUE           Mon         Oct 29         Tokens         M2 DUE           Mon         Oct 29         Tokens         A3 DUE           Oct 31         Certificates         A3 DUE           Vultorization         A3 DUE           Ott 32         Certificates         A3 DUE           Vultorization         A 3 DUE           Mon         Nov 5         DAC         (Schneider, Ch. 7.3]           Med         Nov 5         DAC         [Schneider, Ch. 7.3]         Bishop, Ch. 14.2]         T3 DUE           11         Mon         Nov 12         MLS         [Bishop, Ch. 5-6.2]         M3 DUE           Vultorization         Information Flow         [notes]         M3 DUE           Vultorization         Information Flow         [notes]           Wed         Nov 10 <th< td=""><td rowspan="2">6</td><td>Mon</td><td>Oct 8</td><td>Protocol Design</td><td></td><td></td></th<>	6	Mon	Oct 8	Protocol Design		
Authentication         Wed       Oct 17       Human Authentication       [Schneider, Ch. 5]       T2 DUE         Mon       Oct 22       Fall Recess, No Class       M2 DUE         Wed       Oct 24       Passwords       M2 DUE         Mon       Oct 29       Tokens       M2 DUE         Wed       Oct 21       Certificates       A3 DUE         Authorization         10       Mon       Nov 5       DAC       [Schneider, Ch. 7.3]       (Bishop, Ch. 14.2)       T3 DUE         10       Mon       Nov 5       DAC       [Schneider, Ch. 7.3]       (Bishop, Ch. 14.2)       T3 DUE         10       Mon       Nov 5       DAC       [Schneider, Ch. 7.3]       (Bishop, Ch. 14.2)       T3 DUE         11       Mon       Nov 12       MLS       [Bishop, Ch. 5-6.2]       M3 DUE         12       Mon       Nov 13       IFC (cont'd)       [notes]       [Sabelfeld-Sands]       M3 DUE         Audit         Index Side Side Side Side Side Side Side Side		Wed	Oct 10	Key Management		A2 DUE
WedOct 17Human Authentication[Schneider, Ch. 5]T2 DUE8 MonOct 22Fall Recess, No ClassM2 DUEWedOct 24PasswordsM2 DUE9 WedOct 31CertificatesA3 DUE7WedOct 31CertificatesA3 DUE10 WedNov 5DAC[Schneider, Ch. 7.3]10 WedNov 7Capabilities[Schneider, Ch. 7.3]T3 DUE11 WedNov 12MLS[Bishop, Ch. 5-6.2]T3 DUE11 WedNov 14Information Flow[notes]M3 DUE12 WedNov 13IFC (cont'd)[notes]M3 DUE13 WedNov 26LogsIdgsT4 DUE14 WedNov 28BlocknainsT4 DUE14 WedDec 3Network Security[notes]15 MonDec 10Privacy[notes]	7	Mon	Oct 15	Applied Cryptography		
Mon         Oct 22         Fall Recess, No Class         M2 DUE           Wed         Oct 24         Passwords         M2 DUE           9         Mon         Oct 29         Tokens         A3 DUE           9         Wed         Oct 31         Certificates         A3 DUE           10         Mon         Nov 5         DAC         [Schneider, Ch. 7.3]         T3 DUE           10         Mon         Nov 7         Capabilities         [Schneider, Ch. 7.3]         T3 DUE           11         Mon         Nov 12         MLS         [Bishop, Ch. 5-6.2]         T3 DUE           11         Mon         Nov 12         MLS         [Bishop, Ch. 5-6.2]         M3 DUE           12         Mon         Nov 19         IFC (cont'd)         [notes]         M3 DUE           12         Mon         Nov 19         IFC (cont'd)         [notes]         T4 DUE           13         Mon         Nov 26         Logs         T4 DUE           Verd         Nov 28         Blockchains         T4 DUE           Verd         Dec 3         Network Security         [notes]           Verd         Dec 5         Web Security         [notes]         M4 DUE<				Authent	ication	
WedOct 24PasswordsM2 DUE9MonOct 29TokensA3 DUE9WedOct 31CertificatesA3 DUENuthorization10MonNov 5DAC[Schneider, Ch. 7.3]10MonNov 7Capabilities[Schneider, Ch. 7.3]11MonNov 12MLS[Bishop, Ch. 5-6.2]12MonNov 14Information Flow(notes]12MonNov 19IFC (cont'd)(notes)14MonNov 26LogsT4 DUE14MonDec 3Network Security[notes]14MonDec 3Network Security[notes]15MonDec 10Privacy[notes]		Wed	Oct 17	Human Authentication	[Schneider, Ch. 5]	T2 DUE
9MonOct 29Tokens9WedOct 31CertificatesA3 DUEAuthorization10MonNov 5DAC[Schneider, Ch. 7.3]10MonNov 7Capabilities[Schneider, Ch. 7.3]11MonNov 12MLS[Bishop, Ch. 5-6.2]12MonNov 14Information Flow[notes]12MonNov 19IFC (cont 'd)[notes]14MonNov 28BlockchainsT4 DUE14MonDec 3Network Security[notes]15MonDec 10Privacy[notes]	8	Mon	Oct 22	Fall Recess, No Class		
WedOct 31CertificatesA3 DUEAuthorization10MonNov 5DAC[Schneider, Ch. 7.3]10MonNov 7Capabilities[Schneider, Ch. 7.3]11MonNov 12MLS[Bishop, Ch. 5-6.2]12MonNov 14Information Flow[notes] [Sabelfeld-Sands]12MonNov 19IFC (cont'd)[notes]14MonNov 26LogsT4 DUE14MonDec 3Network SecurityInotes]15MonDec 3Network Security[notes]15MonDec 10Privacy[notes]		Wed	Oct 24	Passwords		M2 DUE
Authorization         10       Mon       Nov 5       DAC       [Schneider, Ch. 7.3]         10       Mon       Nov 7       Capabilities       [Schneider, Ch. 7.3]       [Bishop, Ch. 14.2]       T3 DUE         11       Mon       Nov 12       MLS       [Bishop, Ch. 5-6.2]       M3 DUE         12       Mon       Nov 14       Information Flow       [notes]       M3 DUE         12       Mon       Nov 19       IFC (cont'd)       [notes]       M3 DUE         13       Mon       Nov 21       Thanksgiving, No Class       Tat DUE         Information Flow       [notes]         Information Flow       [notes]         14       Mon       Nov 26       Logs       Zeg       T4 DUE         Information Flow       [notes]         Information Flow	9	Mon	Oct 29	Tokens		
Mon       Nov 5       DAC       [Schneider, Ch. 7.3]         Wed       Nov 7       Capabilities       [Schneider, Ch. 7.3]       [Bishop, Ch. 14.2]       T3 DUE         11       Mon       Nov 12       MLS       [Bishop, Ch. 5-6.2]         Wed       Nov 14       Information Flow       [notes]       [Sabelfeld-Sands]       M3 DUE         12       Mon       Nov 19       IFC (cont'd)       [notes]       [Montes]       M3 DUE         13       Wed       Nov 21       Thanksgiving, No Class		Wed	Oct 31	Certificates		A3 DUE
Wed         Nov 7         Capabilities         [Schneider, Ch. 7.3]         [Bishop, Ch. 14.2]         T3 DUE           11         Mon         Nov 12         MLS         [Bishop, Ch. 5-6.2]           Wed         Nov 14         Information Flow         [notes]         [Sabelfeld-Sands]         M3 DUE           12         Mon         Nov 19         IFC (cont'd)         [notes]         [Montes]         M3 DUE           12         Mon         Nov 21         Thanksgiving, No Class	Authorization					
Mon         Nov 12         MLS         [Bishop, Ch. 5-6.2]           Wed         Nov 14         Information Flow         [notes]         [Sabelfeld-Sands]         M3 DUE           12         Mon         Nov 19         IFC (cont'd)         [notes]           Wed         Nov 21         Thanksgiving, No Class         Technology         Technology           Audit           Technology         Technology           Mon         Nov 26         Logs         Technology         Technology           Mon         Nov 26         Blockchains         Technology         Technology           Augital Security           Interview           Mon         Dec 3         Network Security         [notes]           Interview           Interview <td rowspan="2">10</td> <td>Mon</td> <td>Nov 5</td> <td>DAC</td> <td>[Schneider, Ch. 7.3]</td> <td></td>	10	Mon	Nov 5	DAC	[Schneider, Ch. 7.3]	
Wed         Nov 14         Information Flow         [notes]         [Sabelfeld-Sands]         M3 DUE           12         Mon         Nov 19         IFC (cont'd)         [notes]		Wed	Nov 7	Capabilities	[Schneider, Ch. 7.3] [Bishop, Ch. 14.2]	T3 DUE
12     Mon     Nov 19     IFC (cont'd)     [notes]       13     Mon     Nov 26     Logs       13     Mon     Nov 26     Blockchains       Audit       T4 DUE       Mon     Nov 26       Mon       Mon     Dec 3     Blockchains       T4 DUE       Mon     Dec 3       Mon     Dec 3     Network Security       Mon     Dec 5     Web Security     [notes]       15     Mon     Dec 10     Privacy	11	Mon	Nov 12	MLS	[Bishop, Ch. 5-6.2]	
Wed     Nov 21     Thanksgiving, No Class       Audit       13     Mon     Nov 26     Logs       Wed     Nov 28     Blockchains     T4 DUE       Applied Security       14     Mon     Dec 3     Network Security     [notes]       15     Mon     Dec 10     Privacy     [notes]		Wed	Nov 14	Information Flow	[notes] [Sabelfeld-Sands]	M3 DUE
Audit         Audit         13       Mon       Nov 26       Logs         Wed       Nov 28       Blockchains       T4 DUE         Applied Security         Interstand         Mon       Dec 3       Network Security       [notes]         Wed       Dec 5       Web Security       [notes]         15       Mon       Dec 10       Privacy       [notes]	12	Mon	Nov 19	IFC (cont'd)	[notes]	
Mon       Nov 26       Logs         Wed       Nov 28       Blockchains       T4 DUE         Applied Security         14       Mon       Dec 3       Network Security       Inotes]         15       Mon       Dec 10       Privacy       Inotes]		Wed	Nov 21	Thanksgiving, No Class		
Wed         Nov 28         Blockchains         T4 DUE           Applied Security           14         Mon         Dec 3         Network Security         [notes]           Wed         Dec 5         Web Security         [notes]         M4 DUE           15         Mon         Dec 10         Privacy         [notes]         M4 DUE				Aud	dit	
Applied Security         14       Mon       Dec 3       Network Security       [notes]         Wed       Dec 5       Web Security       [notes]       M4 DUE         15       Mon       Dec 10       Privacy       [notes]	13	Mon	Nov 26	Logs		
14         Mon         Dec 3         Network Security         [notes]           Wed         Dec 5         Web Security         [notes]         M4 DUE           15         Mon         Dec 10         Privacy         [notes]		Wed	Nov 28	Blockchains		T4 DUE
Wed         Dec 5         Web Security         [notes]         M4 DUE           15         Mon         Dec 10         Privacy         [notes]						
15 Mon Dec 10 Privacy [notes]	14	Mon	Dec 3	Network Security	[notes]	
		Wed	Dec 5	Web Security	[notes]	M4 DUE
Wed         Dec 12         Trusted Hardware         [notes]	15	Mon	Dec 10	Privacy	[notes]	
		Wed	Dec 12	Trusted Hardware	[notes]	

#### Countermeasures

A defense that protects against attacks by neutralizing either the threat or vulnerability involved

Strategy:

- Prevent: block attack or close vulnerability Prevention
- Deter: make attack harder
- Deflect: make other targets more attractive
- Mitigate: make harm less severe
- Detect: as it happens or after the fact
- Recover: undo harm

Risk Management

Deterrence
through
Accountability

#### **Principles of Prevention**

[Saltzer and Schroeder, *The Protection of Information in Computer Systems*, 1975]

- Accountability
- Complete Mediation
- Least Privilege
- Failsafe Defaults
- Separation of Privilege
- Defense in Depth
- Economy of Mechanism
- Open Design
- Psychological Acceptability

#### Accountability

#### Hold principals responsible for their actions



# Accountability

Hold principals responsible for their actions

- Authorization: mechanisms that govern whether actions are permitted
- Authentication: mechanisms that bind principals to actions
- Audit: mechanisms that record and review actions





# Accountability

Hold principals responsible for their actions

- <u>Au</u>thorization: mechanisms that govern whether actions are permitted
- <u>Au</u>thentication: mechanisms that bind principals to actions
- <u>Audit</u>: mechanisms that record and review actions
   ... Gold Standard [Lampson 2000]







#### **Complete Mediation**

Every operation requested by a principal must be intercepted and determined to be acceptable according to the security policy



#### **Complete Mediation**

Every operation requested by a principal must be intercepted and determined to be acceptable according to the security policy

- Component that does the interception and determination is the reference monitor
- Related to Accountability
- Restricts caching of information, including previous decisions

#### Least Privilege

Principals should be given the minimum privileges necessary to accomplish their task

- Limits the damage that can result from accident or malice
- Cf. "need to know"

#### Failsafe Defaults

Base decisions on the presence of privilege, not the absence of prohibition

The default answer is "no"



- Say "yes" only when there is an explicit reason to do so
- Principals who discover they don't have access will complain
- Attackers who discover they do have access won't complain!

#### Failsafe Defaults

#### Java stack inspection circa 1998:

```
checkPermission(T) {
  // loop newest to oldest stack frame
  foreach stackFrame {
    if (local policy forbids access to T by class executing in
        stack frame) throw ForbiddenException;
    if (stackFrame has enabled privilege for T)
      return; // allow access
    if (stackFrame has disabled privilege for T)
      throw ForbiddenException;
  }
  // end of stack
  if (Netscape | ...) throw ForbiddenException;
  if (MS IE4.0 | JDK 1.2 | ...) return;
}
```

#### Separation of Privilege

- Different operations should require different privileges
- Disseminate privileges for an operation amongst multiple principals (Separation of Duty)





#### Defense in Depth

Prefer a set of complementary mechanisms over a single mechanism

Complementary:

- Independent: attack that compromises one mechanism is unlikely to compromise others
- Overlapping: attacks must compromise multiple mechanisms to succeed



#### Exercise

 Consider the security mechanisms deployed in your dorm and/or in academic buildings on campus.
 These systems are designed to prevent access by unauthorized people.



- To what extent do those security features enforce Complete Mediation?
- To what extent do those security features enforce Least Privilege?
- To what extent do those security features satisfy the independence requirement of Defense in Depth?
- To what extent do those security features satisfy the overlapping requirement of Defense in Depth?

#### Economy of Mechanism

Prefer mechanisms that are simpler and smaller

- Easier to understand, construct, analyze
- Hence less likely to have unknown vulnerabilities
- Applies to any aspect of system, not just security

Trusted computing base (TCB): mechanisms that implement the core security functionality ...keep the TCB small

# **Open Design**

Security shouldn't depend upon the secrecy of design or implementation



# **Open Design**

Security shouldn't depend upon the secrecy of design or implementation

#### **Arguments for open design:**

- Secrets eventually come out: reverse engineering is possible, employees move around
- Making details public increases chance of identifying and repairing vulnerabilities

# **Open Design**

Security shouldn't depend upon the secrecy of design or implementation

#### **Arguments against open design:**

- Secrecy supports Defense in Depth by making it harder to find vulnerabilities
- Lack of hard evidence that Linus' Law really holds ("given enough all eyeballs, all bugs are shallow")
- After identification, some vulnerabilities cannot quickly or easily be repaired

#### **Psychological Acceptability**

Minimize the burden of security mechanisms on humans

- Don't make operations (much) more difficult to complete than if security mechanisms were absent
- Don't make configuration difficult
- Produce comprehensible error messages

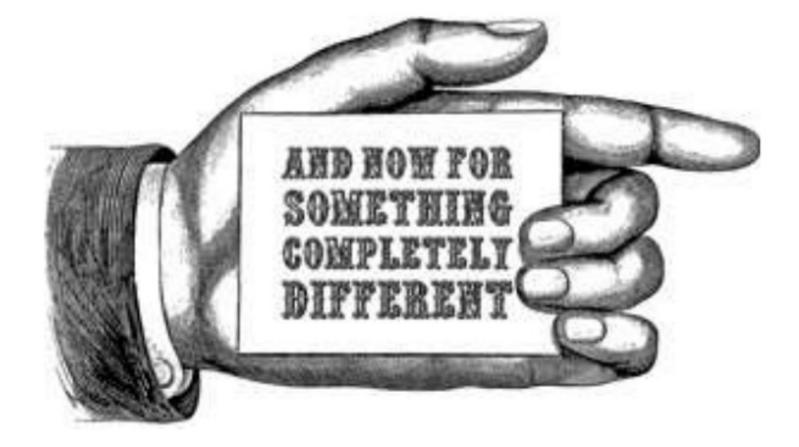
...always a tradeoff between security and usability

#### Alternative su

- A student who didn't take 181S decides to build a new version of su that works as follows:
  - If the open operation succeeds, then the password is checked. If it is indeed the correct password for u2, then u1 is granted access to the account of u2.
  - If the open operation fails, then u1 immediately is granted access to the account of the superuser ("root"). The student's intention is that u1 would then be able to fix the misconfiguration.

### **Principles of Security**

- Accountability
- Complete Mediation
- Least Privilege
- Failsafe Defaults
- Separation of Privilege
- Defense in Depth
- Economy of Mechanism
- Open Design
- Psychological Acceptability



#### What skills will your project need?

#### Forming a group...

- What skills/experience will you bring to a group?
- What system(s) are you exciting about building?
- How challenging do you want your project to be?
- How often/when are you available to meet?