INST0031
Systems Management

Lecture 7

Security Tools

What we will cover today

- Security
  - What are we talking about?
  - Mechanisms
    - Encryption
    - A few application specifics
- Legal requirements and considerations
  - Privacy, Accuracy, Intrusion
- Some scary thoughts...

System security controls

- Against what?
  - Unauthorised access
  - Unauthorised use
  - Accidental damage
  - Malicious damage

External and internal access control

- Login control – IDs and passwords
- Access control – rights, flags, options, etc.
- Terminal restrictions
  - User to terminal
  - Activity to terminal
- Time restrictions
- Lockouts & alarms

Information structure

- How will the information be accessed?
- How will the information be used?
- Back to basic design:
  - Workgroups
  - Systems Analysis
  - Workflows
- Design directory structures with security in mind.

Access permissions

- The System Supervisor
- Backdoor entry
- User groups/classes
- Equivalences

Rights

- Hierarchies of rights
- Rights profiles
  - System rights
  - Personal rights
  - Group rights
  - Directory rights
  - File rights

Flags/Attributes:

- What are flags and attributes?
- Common types of attribute:
  - search
  - read
  - write/modify
  - create
  - delete
  - execute
  - parent
  - change attributes

Security problems and solutions

- Causes of system security breaches
  - Misrepresentation
  - Illicit capture of information
  - Viruses
- The fundamental issues
  - Authentication
  - Secure transmission
    - Encryption
  - Management

Authentication

- Who are you? - Logins
- Who did you say you were?
  - PIN authentication
  - Token authentication
  - Subverting authentication
    - Assumptions of honesty
    - Sniffing
    - Vulnerability of unencrypted systems
- Advanced systems
  - Distributed Security Systems

Kerberos

- Developed at MIT for network security
- Allows client to "prove" identity to a server, and vice-versa, across an insecure network
- Uses strong cryptography
  - Based on temporary cryptographic key exchange
  - Handled by use of Tickets
    - TGTs and TGSs

Tickets

- TGT – Ticket Granting Ticket
  - When a user first authenticates, the Key Distribution Centre (KDC) gives a TGT encrypted with the user's password
- TGS – Ticket Granting Service
  - When the user wants to use a Kerberised service, the TGT allows the user to talk to the TGS which verifies ID with the TGT and issues a new, specific ticket for the requested service

Tickets

- This approach, whilst seemingly complicated, has two big benefits:
  - The user only has to authenticate once (doesn't have to keep re-entering password – more convenient and less chance of capture)
  - If a ticket is compromised the risk window is limited as it expires with the ticket.
- For a "simple" ☺ explanation of protocol: web.mit.edu/kerberos/www/dialogue.html

TLS (SSL)

- Transport Layer Security
  - Development of SSL (Secure Sockets Layer)
  - HTTPS uses HTTP + TLS/SSL
- Focused on Web security
- Idea to provide security at the Transport layer
- Authenticates workstation rather than user
- A less secure/complete solution?

Cryptography

- Cryptography is a Greek word:
  - Crypto: Secret
  - Graphy: Writing
  - To send messages that are only readable by the expected recipient.

- The key concept
  - Encryption to encode
  - Decryption to decode
- Symmetric and Asymmetric keys

Some terminology

- Cryptography: Transform the messages and communication into a protected form
- Cryptanalysis: Try to break the code and understand the message
- Plaintext: The original message
- Ciphertext: Transformed message
- Encryption: Transforming plaintext to ciphertext
- Decryption: Transforming ciphertext to plaintext

Cipher vs Code

- Cryptography uses cipher rather than code.
  - A cipher is a character-for-character or bit-for-bit transformation (without linguistic structure)
  - A code replaces one word with another word or symbol
- Example
  - A cipher: attack → DWWDFN
  - A code: antitank weapon → tortoise killer

Traditional Encryption

- Substitution Cipher: replaces each letter by another one. It preserves the order of the plaintext symbols but disguises them.
- Transposition Cipher: reorders the letters but does not disguise them.

Substitution Cipher (1)

- Caesar Cipher: replace each letter by another one which is 3 letters away.
  - Replace A by D, B by E and …

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Example :
  - Plaintext: attack
  - Ciphertext: dwwdfn

Substitution Cipher (2)

- Shift Cipher : replace each letter by another one which is n letters away.
  - n can be maximum 26

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Example : n=5
  - Plaintext: attack
  - Ciphertext: fyyfhp

Substitution Cipher (3)

- Mapped Cipher : a designated replacement for each letter (MY MADE-UP NAME)

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

- Example :
  - Plaintext: attack
  - Ciphertext: QZZQEA

Substitution Cipher (4)

- Vigenere Cipher : Using a key to find the substitution cipher, which is not always the same for one exact plaintext

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51

- Example :
  - Plaintext: attack at the dawn on the front line of the enemy
  - Key: ORANGE
  - Ciphertext: ?

Substitution Cipher (4)

- Vigenere Cipher: encrypt

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51

- Plaintext: attack at the dawn on the
- Key: ORANGE
- Ciphertext: OKTNIO OK TUK HONN BT XVV

a	t	t	a	c	k		a	t		t	h	e		d	a	w	n		o	n		t	h	e	
O	R	A	N	G	E		O	R		A	N	G		E	O	R	A		N	G		E	O	R	
O	K	T	N	I	O		O	K		T	U	K		H	O	N	N		B	T		X	V	V	

Substitution Cipher (5)

- Vigenere Cipher: decrypts

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51

- Ciphertext: OKTNIO OK TUK HONN BT XVV
- Key: ORANGE
- Plaintext: attack at the dawn on the

O	K	T	N	I	O		O	K		T	U	K		H	O	N	N		B	T		X	V	V	
O	R	A	N	G	E		O	R		A	N	G		E	O	R	A		N	G		E	O	R	
a	t	t	a	c	k		a	t		t	h	e		d	a	w	n		o	n		t	h	e	

Different Types of Substitution Cipher (1)

- Monoalphabetic Cipher : The general system of symbol-for-symbol substitution. One plaintext letter is always the same ciphertext letter.
- Makes it weak to break, the basic attack takes advantage of the statistical properties of natural languages, in English:
  - The most common letter is e, followed by t, o, a, n, i, etc.
  - The most common two-letter combinations, or digrams, are
- th, in, er, re, and an.
  - The most common three-letter combinations, or trigrams, are the, ing, and, and ion.

Different Types of Substitution Cipher (2)

- Poly-alphabetic Cipher : Different symbols substitution for different positions of the same plaintext letter/symbol. One plaintext letter can become different ciphertext letters.
- Uses a text based key and modulo arithmetic to perform the encryption

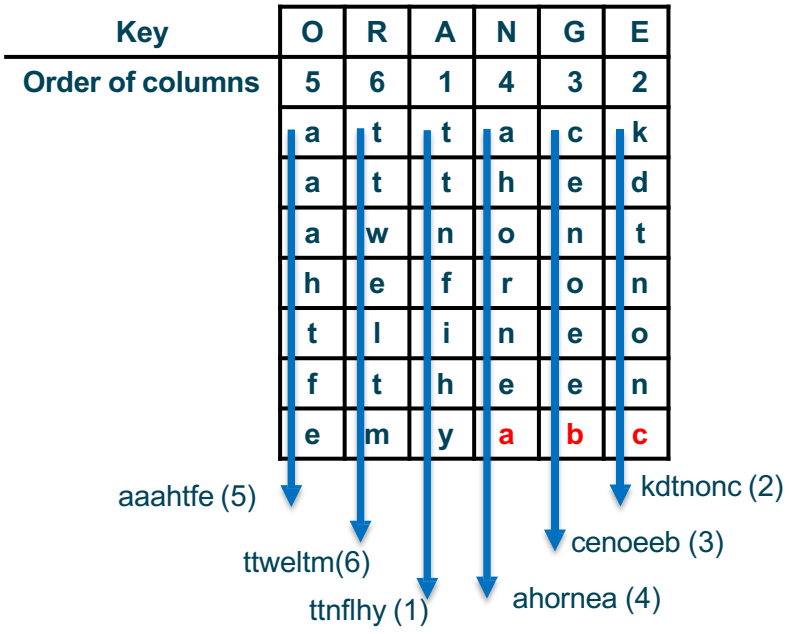
Transposition Cipher (1)

- Columnar Transposition Cipher: keyed by a word or phrase not containing any repeated letters.
- Example :
  - Plaintext: attack at the down on the front line of the enemy
  - Key: ORANGE
  - Ciphertext: ?

Key	O	R	A	N	G	E
Order of columns	5	6	1	4	3	2

Transposition Cipher (2)

- Columnar Transposition Cipher: encrypt:
  - Plaintext: attack at the dawn on the front line of the enemy



1. ttnflhy
2. kdtnonc
3. cenoeeb
4. ahornea
5. aaahtfe
6. ttweltm

NOTE: to avoid giving any information about the key remove the spaces from ciphertext.

Ciphertext: ttnflhykdtnonccenoeebahorneaaaahtfettweltm

Transposition Cipher (3)

- Columnar Transposition Cipher: decrypt:
  - Ciphertext: ttnflhykdtnonccenoeebahorneaaaahtfettweltm
  - Key : ORANGE à 6
  - Number of characters in Ciphertext= 42
  - Number of chars in each column = 42/6 = 7
  - Ciphertext: ttnflhy / kdtnonc / cenoeeb / ahornea / aaahtfe / ttweltm
  - Look at the key to identify the sequence of each section:
    - O(5) R(6) A(1) N(4) G(3) E(2)

Transposition Cipher (4)

- Columnar Transposition Cipher: decrypt:

Key	O	R	A	N	G	E
Order of columns	5	6	1	4	3	2
	a	t	t	a	c	k
	a	t	t	h	e	d
	a	w	n	o	n	t
	h	e	f	r	o	n
	t	l	i	n	e	o
	f	t	h	e	e	n
	e	m	y	a	b	c

Plaintext:
attackatthedawnonthefrontlineoftheene myabc

Attack at the dawn on the front line of the enemy abc.

Two Fundamental Cryptographic Principles

- Redundancy: all encrypted messages must contain some redundancy, that is, information not needed to understand the message.
  - Cryptographic principle 1: Messages must contain some redundancy
- Freshness: measures must be taken to ensure that each message received can be verified as being fresh, that is, sent very recently.
  - Cryptographic principle 2: Some method is needed to foil replay attacks

Modern Encryption

- The same basic ideas as traditional cryptography (transposition and substitution) but Different emphasis.
- Traditionally, cryptographers have used simple algorithms, emphasis on the key.
- Nowadays, the objective is to make the encryption algorithm too complex and involuted to be impossible to break without the key.

Symmetric Key

- Symmetric Key: use the same key for encryption and decryption
  - Stream Cipher: plaintext is substituted or transpositioned bit-by-bit or byte-by-byte into ciphertext
  - Block Cipher: a block of plaintext is substituted or transpositioned into cipher text.

- Key exchange is the shortcoming of this method.

Asymmetric Key (1)

- Asymmetric Key: the encryption and decryption keys were so different that the decryption key could not feasibly be derived from the encryption key. (Also known as public key/ private key)
- Three requirements:
- – D(E(P)) = P.
  - It is exceedingly difficult to deduce D from E.
  - E cannot be broken by a chosen plaintext attack.

Asymmetric Key (2)

- A key-pair to encrypt by any sender and decrypt by the specific receiver. They are mathematically linked together.
- Public key: Everyone knows it and uses it for encryption.
- Private key: It is a private and secret key to be used for decryption.

Digital Signature

- Digital Signature: is a proof of ownership of a public key. Issued by Certification Authorities.
  - Authentication: Only authorised entities can decrypt the message
  - Integrity: The message is not altered or changed.
  - Non-repudiation: It is clear who the sender is and they can't deny or change the message.

Pretty Good Privacy…

- The concept of two-key encryption
  - Single Secret keys vs Public and Private keys
  - RSA (Rivest-Shamir-Adelman)
    - To multiply two huge prime numbers is easy…
    - To find two prime factors is not!
  - Security levels and crackability
- In practice, effective basic security and authentication combined

Viruses

- Already addressed
- Viruses in the real world
  - A new form of terrorism?

Cyber warfare

Stuxnet: Anatomy of a Computer Virus

- An infographic dissecting the nature and ramifications of Stuxnet, the first weapon made entirely out of code.
- http://vimeo.com/25118844
- This was produced for Australian TV program HungryBeast on Australia's ABC1
- CBS 60 minutes
  - http://www.youtube.com/watch?v=kw--zLJT3ak
- Further Developments
  - http://www.securityweek.com/first-stuxnet-victims-unmasked-research

Hacking and Cracking

- An old form of terrorism!
- Often more low-tech than high-tech
- High-tech approaches spottable
- Loopholes
- Another people problem
- Spoofing
- Anonymous mailers
- No such thing as a secure system

Firewalls

- Protection by isolation
- The firewall concept
- Proxy service
- 2-way control
- Net nannys
- What about internal threats?

Other considerations

- The Majors vs Little League
  - Industrial espionage
  - Technological dependency
  - Coverups and conspiracy
- Neverending problems of security
  - The Ping of death
  - Software vulnerability
- No such thing as a secure system – again!

Social Issues (1)

- Privacy & Freedom of speech:
  - People have a right to privacy. However the nature of internet has made it easier for governments and bad actors to spy on citizens.
  - It is also easier for citizens to use cryptography to prevent this spying.
  - Real privacy means it is much harder for governments to spy on criminals of all stripes, but it is also harder to spy on journalists and political opponents.
  - Some governments restrict or forbid the use of cryptography

Social Issues (2)

- Privacy & Freedom of speech:
  - Related to privacy is freedom of speech.
  - Depending on the nature of a regime, governments want to limit their citizen's access to certain information.
  - Cryptography allows people to hide their browsing habits and communications from governments.
  - Though Cryptography is essential to many daily activities such as banking, healthcare communication and many more, it may cause obstacles to identify and monitor illegitimate activities.

Security Policies

- A security policy is essentially a document stating security goals, and which actions are required, which are permitted and which are allowed.
  - Policies may apply to actions by a system, by management procedures, by employees, by system users.
  - A complete security policy is a collection policies on specific security issues.
- Do not confuse a policy with an enforcement mechanism
  - Every security policy statement should have a corresponding enforcement mechanism
  - The enforcement mechanism may be a technology (e. g., a firewall), or a process (e. g., security audit)

Challenges in Security Policies

- Extremely difficult to develop
- Unique to each organization.
- No common format or process for developing one.
- Making it simple so everyone can understand and use it.
- Getting management consensus.
- How do you enforce it?

Basic Policy Requirements for Employees

- Policies must:
  - Be implementable and enforecable
  - Be concise and easy to understand
  - Balance protection with productivity
- Policies should:
  - State reasons why policies are needed
  - Describe what is covered by the policies
  - Define contacts and responsibilities
  - Discuss how violations will be handled

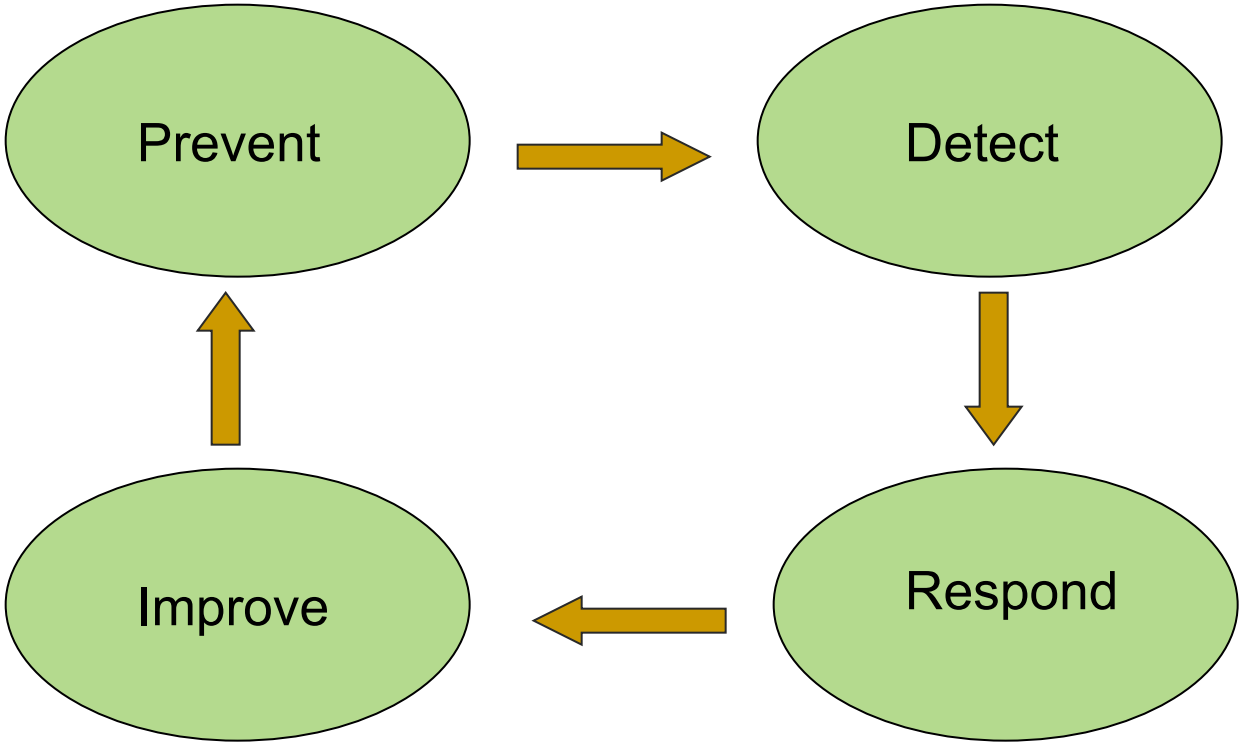
Basic Security Policy Process

- Identify what assets you need to protect
- Identify the vulnerabilities and threats to those assets
- Identify the risks of threats exploiting the vulnerabilities
- Establish countermeasures to mitigate the threats
  - Policies and procedures
  - Technical controls
  - Human controls
- Monitor compliance and effectiveness of controls (Metrics)
- Periodically review and update controls

Training and Awareness

- Once approved and disseminated throughout organization:
  - Train and educate ALL employees
  - Have everyone sign
  - Begin enforcement immediately
- Accomplish non-personnel related actions
- Security personnel must constantly assess viability

Security Modules



Elements of a Comprehensive Security Program

- ✓ Have good passwords
- ✓ Use good updated antiviral products
- ✓ Use strong cryptography
- ✓ Proper use of firewalls and IDS
- ✓ Have a backup-system
- ✓ Audit and monitor systems and networks
- ✓ Test your security frequently
- ✓ Have training and awareness programs

ALL AS PART OF A SECURITY POLICY

Conclusions

- Information security costs but if not implemented there are many risks:
  - Inability or impairment of a company's ability to perform its objectives.
  - Inability to provide needed services to the public.
  - Waste, loss, abuse or misappropriation of funds.
  - Loss of credibility or embarrassment to your company.
  - Company competition gain upper hand by stealing confidential information from your server.
  - Decreased profit, and increase loss margin.
  - Client trust relationship tarnished.

Conclusions

- Information security is not an easy task within an organization
  - It is a continuous process
  - Requires constant auditing
  - Requires constant education

- Information security is like a chain; it is only as strong as the weakest link

Sources of information

- Electronic Frontier Foundation - www.eff.org
- FAS Information warfare and security - www.fas.org/irp/wwwinfo.html
- Searchsecurity.com - searchsecurity.techtarget.com
- Insecure.org - www.insecure.org
- The War room - www.warroom.com
- alt.conspiracy? :-) groups.google.com/forum/#!forum/alt.conspira

Useful reading

- http://www.pgpi.org/doc/pgpintro
  - Very readable document from PGPI which explains not only PGP but all the fundamentals of cryptography in easy-to-understand language
- http://web.mit.edu/kerberos/www/dialogue.html
  - As previously mentioned, a mock Euripidean dialogue which explains the fundamental reasoning and principles behind Kerberos and ticketing systems. Particularly recommended for classicists :-)

Questions?