Active Content, E-commerce, Mobile and Convergence Security

Topics

- What is executable content
  - Mostly WWW-related
- How to secure e-commerce
- Convergence of Telecoms and Internet
- Smart Cards

Executable Content

- Data is received from some outside source and executed as a program on the client host
  - Automatic execution
  - Usually received from a WWW page
- Executable content is a potentially powerful technology and keeps on appearing in different forms
  - Agents
  - Active networks
  - Proxlets
- But it changes the security picture
  - One moment it is data, the next it is program

Problems With Executable Content

- Computation is moved to the client
- The problem area is related to malware
- Clients need to be protected from rogue service providers
- End users are forced to become administrators and policy makers
- Mobile (agent) code moves from host to host, executing a task given to it
  - Clients must be protected from malicious mobile applications
  - The mobile code must be protected from a malicious host

What to trust

- Code origin
  - Local code is trusted
  - Remote code is not trusted
  - Implemented by e.g. Java
- Signed Code
  - Code is signed
    - Carries a certificate
    - Usually requires a PKI
  - Implemented by e.g. ActiveX, Java
  - Signature is proof of source, but not proof of non-malicious intent
- Other approaches
  - Known code: hash/checksum can be used to protect the code from being changed
  - Proof carrying code: a research approach, still not working in practice

ActiveX

- Idea of small controls, i.e. functional components
  - Buttons, labels, charts etc
- For the Windows/Internet Explorer environment
- Loaded from disk, if not there fetched from the net
  - An ActiveX component is signed by a vendor and the signature is checked by the client software using an included certificate and PKI structure
- What about signed but malicious controls?
  - Examples can be found

ActiveX Authenticode

- Microsoft's solution for securing executable content
- Code is signed
- Browser asks user whether to allow the downloaded code to run or not
- If the user accepts the certificate, the software is allowed to run without any restrictions
  - It could delete all your files
- Problem: users often want to try a program even if they do not trust its source

Java

- Sun Java technology
- Java is many things
  - An object oriented programming language
  - Run time environment
- Client executable code is called an applet
- Applets may come from any source
- Users may want to securely run code they do not trust (they might not even know where it came from)
- The Java programming language was designed with security in mind
  - Byte code verifier, class loader & security manager
- Implementations in browsers have had serious bugs

Security Model of a Java Applet

- Java is a general purpose language, here we are looking at applet use
- Classloader in the run time environment differentiates between local (trusted) and network (applet) code
  - Local class is (should be) always preferred to network class
- Verifier checks the byte code
  - Byte code is the binary code compiled from the Java source code and native to the Java Virtual Machine
  - The Verifier attempts to find stack over and under flows, checks correct use of variable types and generally the syntax of the byte code
- SecurityManager implements the Java sandbox
  - Sandbox limits the applet's actions severely

The Java Sandbox

- The applet in the sandbox may not:
  - Read or write files
  - Open network connections to hosts other that the originating host
  - Initiate execution of new processes or programs
  - Use any native methods
- Only trusted code (local classes) can use the OS services
  - Local library classes check if they are called from the sandbox or from a local applet running outside the sandbox
- Signed applets can exceed the sandbox limitations

Javascript

- Not related to Java
- Also called ECMAScript
- Microsoft calls its version Jscript
- A scripting language created by Netscape used in Web pages
  - A higher level language than Java or ActiveX
- Some sandbox-like security features
  - Intended to be secure enough for browser use
- Bugs have been found

Other Browser Add-ons

- Flash, Shockwave, Acrobat (PDF reader), video codecs etc.
- Software components added to the browser program
- Often contain a relatively powerful language
- Usually designed to be "safe"
- Have been found to contain many vulnerabilities

Server Side Code

- Server side code is executed in the server
  - Bugs can compromise the server (intrusions)
  - Execution requires computational resources from the server (denial of service)
  - Client (browser) side security is not directly impacted by the server side code
- Server side code can be in any language
  - Java, PHP, C, Shell scripts etc.
- Server software requirements have been discussed
- Systems administrators should be wary of letting ordinary users write their own code
  - Many scripts are written by people who know little or nothing about security

Security Models for Distributed Systems

- The previously presented formal models are not wholly obsolete
  - The formal models describe a security policy
- Distributed security can be implemented by defining:
  - PAP, Policy Administration Point
  - PDP, Policy Decision Point
  - PEP, Policy Enforcement Point
  - PIP, Policy Information Point
- Thus a policy is created at PAP (admin. workstation) and when a PEP (firewall) sees a new traffic flow request (TCP connection) it requests the PDP (a server) for a decision. The PDP asks the PIP for additional information (which user is using the host that PEP says the traffic is from) and makes a decision.

Securing E-commerce

- E-commerce is an application over some infrastructure, like the Internet
- As an application it has several security needs
  - Security of the serving infrastructure technology
  - Security of the information in the server
  - Security of the transaction
  - Non-repudiation needs

Types of E-Commerce

- Business to Business
  - Typically medium size to large transactions and long term relationships
- Business to Consumer
  - Typically small to medium size transactions and loose relationships
- Consumer to Consumer
  - Typically small to medium size transactions, lack of trust between the parties and no prior relationships
- Different types of commerce prefer different solutions

E-Commerce Servers

- WWW and e-mail are the most common applications
- Standard firewall and host security solutions can be used to secure the server
- The server often contains credit card information, customer addresses, business confidential data, pending orders etc.
  - Some credit card companies already require that the credit card information is located in a separate server
    - Front and back-end server architecture
  - Threatens both to confidentiality and integrity

E-commerce Transactions

- Identifying the participants is often required
  - SSL authenticates the server
  - PKI systems could be used to authenticate both participants (once they are in global use)
  - PGP and S/MIME could be used, but are rarely used
  - Extranets can use PKI or usernames and passwords
  - Sometimes it is easiest to accept a certain amount of losses
- There are formal standards for B2B commerce
  - EDI/OVT
  - XML-based standards are emerging
  - PKI-based signatures are beginning to be used

TEKNILLINEN KORKEAKOULU

Non-repudiation in E-commerce

- PKI systems could provide electronic signatures
  - Many countries have laws about these
- What happens if the signer repudiates the signature?
  - The whole system may be evaluated in public court
- Transaction logs can be useful
- Instead of non-repudiation, how about pre-payment
  - In Finland the banks have rather flexible online systems
  - The credit card companies have different solutions, too
  - Remember that WWW forms and cookies are freely editable by the user

Mobility

- A mobile device often lacks a permanent identifier
  - Creates a practical problem, as many communications protocols tie the connection to the IP address of the host
    - A legacy problem, original IMP weighted about 500 kg
  - In theory this is not a problem
- Current solutions:
  - Move mobility to a different domain
    - E.g. mobile telecommunications systems (GPRS, UMTS) hide the mobility, the host has a fixed IP address
  - Use a stationary server to hide the mobility, like Mobile IP
  - Create a new protocol, like HIP, SCTP with its own identifiers

Security for Mobile Telephony

- 1G FDMA analog, ARP, NMT
  - No security for data
  - Phone identified by ID, not verified
- 2G TDMA digital stream, GSM, GPRS
  - Stream encryption for data
  - Symmetric key encryption with a shared secret stored in SIM in phone and HLR database in the network
  - Algorithms are secret (some have been reverse engineered)
- 3G CDMA spread spectrum, UMTS
  - Block encryption for data
  - USIM in phone and AuC (Authentication Center) in the network share a 128 bit secret key

Convergence of Telecommunications and Internet

- Internet and traditional telecommunications networks and services are converging
  - Called NGN, Next Generation Network
- As systems they are very different
  - Telecoms network is one big machine, where all intelligence is in the network
  - Internet is a simple message passing network, where all intelligence is on the edges
- This will cause security problems

Security in Telecom Networks

- Separate user and control planes
  - Misuse very difficult
  - Occasionally possible, e.g. hacking of in-band signaling
- Signaling security
  - Most of the signaling is in a separate network (control plane, implemented using SS7)
- Signaling is truly international
  - Between operators and countries
- Most critical services and components are duplicated
- Bits in telecoms mean money, therefore good security built in

Integration

- Parts or all of the telephone bearer network are being replaced with IP networks
- Internet VoIP calls are routed to the telephone system
  - SIP (Session Initiation Protocol) to initiate the call
- UMTS will have an IPv6 internal network
  - Possibly with virtual operator's equipment
- UMTS will also have the IMS (IP Multimedia Subsystem) to replace MSC (Mobile Switching Center)

Integration and New Problems

- No more user/control plane separation
  - Signaling and user data intermixed
  - Caller's telephone number can no longer be trusted
    - As it is delivered with SIP over the Internet
- Borders and responsibilities between operators blurred
- Terminal equipment much more intelligent
- Networks extended to customer premises
  - Physical protection not any more the same

TEKNILLINEN KORKEAKOULU

Future View: Basic Security After Convergence

- Data and Telecom Networks integrated
  - Signaling integrated, accounting combined
  - Signaling protected cryptographically
- Accounting integrated
  - Visonaries say through a millicent system like ecash in order to reduce delay
  - Or flat fee for basic services
- Firewalls everywhere
- User data protected cryptographically
- Management will be a large problem
  - How to manage cryptographic keys?
  - How to manage firewall access control?

Tamper Resistant Hardware

- Problem: hardware is given to end users, but the contents should remain in the control of the owner or originator of the hardware
  - Telephone SIM cards
  - Smart cards (used for access, TV decoders, ID, money...)
  - Cryptographic password tokens (eg. SecurID)
  - Car computers
  - Public ATM machines
- One solution is tamper detection with e.g. seals
  - Especially if the problem domain allows rollback, meaning that the effects of the tampering can be reversed

Smartcards

- A plastic card with a CPU and non-volatile memory
- Can store information and perform low-end processing
- Draws power from the host terminal, often also a clock pulse
- Communicates with the host terminal
- Usually used for authentication
  - The user proves their identity by showing that they have the smart card and know a password (often called PIN)
  - The smart card contains a public key wrapped in a certificate, which is passed to the terminal and can prove that it has the private key when queried
- Suomeksi: toimikortti

Smartcard Attacks

- The data on a smartcard (often a crypto key) can be extracted using several methods
  - Gaining access to the circuitry and by reading the data as it is transferred from the memory to the CPU
    - Requires shaving the protective layers of the card or careful drilling
  - Monitoring the power consumption of the card and deducing the key as it is used by clever mathematics (e.g. Chinese Reminder Theorem)
  - Interrupting the operation of the smart card by tampering with the operating voltages or the clock signal
- With simple money cards it is often enough to prevent change to the memory
  - The attacker can try to filter out the EEPROM write voltage
- Smartcards are getting better all the time, but they are not invulnerable

Future of Security

- Cryptography and PKI are seen currently as the silver bullet to solve all problems
  - PKI is more complex than originally thought
- It has been said that this is the “golden age” of hacking and cracking
  - Current and future systems will have security included from the start of the design process, not as an afterthought
- In the future security services are going to be more clearly defined and easily available
  - Security is an infrastructure service
- However implementing security will continue to require know-how in the foreseeable future

Sample Questions

- T/F, justify:
  - Java is secure, ActiveX is not
    - a: Java has sandbox, ActiveX signed code, might go either way
  - E-commerce requires signatures
    - a: no, signatures add to trust, but have a cost, depends on situation and risk analysis needed
  - Telco networks are inherently more secure than the Internet
    - a: true -> 0p
    - a: true, separation of control and user plane solves many problems -> 1p

Sample Questions

- Design a web store with security in mind (4 p)
  - SSL/TLS for customers, front- and back-end architecture, IDS in between, firewall outside -> 0,5p each mentioned, 1,5 p if discussed, max 3 p
  - Customer authentication no sooner than checkout, employee security screening, processes for handling customer information -> 0,5p each mentioned, 1p if discussed, max 1,5 p
  - Nice picture: 0,5 p
  - Somewhat irrelevant info, like anti-viral software in the Unix-based
    back-end -> no effect
  - Extra info that is obviously not relevant or does not make any sense -> minus points

TEKNILLINEN KORKEAKOULU

Further Studies at TKK

- Internet security:
  - Tuomas Aura, Sasu Tarkoma
  - http://www.cse.tkk.fi/Datacommunications/Studies/
  - http://www.cse.tkk.fi/Datacommunications/Studies/Courses/
- Cryptography:
  - Kaisa Nyberg
  - http://www.tcs.hut.fi/Research/Crypto/
  - T-79.4501 Cryptography and Data Security
  - T-79.5501 Cryptology
  - T-79.5502 Advanced course in cryptology

TEKNILLINEN KORKEAKOULU

T-110 Courses

- T-110.4200/6 Information Security Technology
- T-110.5110/6 Computer Networks II - Advanced Features
- T-110.5140 Network Application Frameworks
- T-110.5200 Laboratory Work on Network Security
- T-110.5211 Cryptosystems
- T-110.5220 Usability and Security
- T-110.5230 Practical Security of Information Systems (hacking)
- T-110.5290 Seminar on Network Security
- T-110.5600 Yritysturvallisuuden perusteet (likely to end)
- T-110.5620 Tietoturvallisuuden kehittämisprosessit (likely to end)
- T-110.6200 Special assignment
- T-110.6210 Individual studies
- T-110.6220 Special Course in Communications Security
  - Malware next spring
  - Network security by Tuomas Aura this fall
- T-110.7xxx courses

- Any course with special or seminar in name has usually variable content and may contain security related topics