

Network Security: State of the Art, Hot Topics

1

The Future?

- Let's hope we make progress in computer security

After all...

... The future is just around the corner! :)

2

What is “Progress”?

- Practical goals
 - Making Ecommerce real
 - Making Ecash work
 - Making systems resist 99+% of attacks
- Fundamental problems
 - Delegation of trust
 - Solving social maladjustment via software
 - Trusting executables / secure executables

3

Defining Progress

- I define “progress” as positive movement toward practical goals
- Analogous to water level in a ship
 - Are you pumping water out faster than you are taking it on?
 - Are you patching holes faster than you’re drilling new ones?
 - ***Do you have time to design the next generation of ships??***

4

The Problem with Progress

- Large enough amounts of progress require violent change (revolution V. evolution) or all we have is dinosaurs
- It may already be too late to fix
 - The Internet is **really huge**; upgrade it?
 - Upgrading the Internet is a problem **on the order of changing the electrical voltage of a first-world country**

5

Learn to See Security as Infrastructure

- A well-designed network is inherently
 - More secure
 - Faster
 - More reliable
 - (Maybe) cheaper to manage
- Retrofitting security into existing networks is a losing game
- Do it right the **first time**

6

The Market

- The security products market is growing rapidly
 - 1) We must deliver solutions that work
 - 2) What are we getting for our money?
 - 3) Is it being well spent?
 - 4) Are there alternatives?

7

Delivery

- Computer security experts have been waving red flags about dangers of Electronic Commerce
 - We've got their attention
 - Now we have to *deliver* or we're on the scrap heap
 - Costs of security must be in line with benefits

8

Costs

- Infosecurity news security survey:

Mean Expenditures:

<u>1994</u>	<u>1995</u>	<u>1996</u>
\$140,000	\$175,000	\$201,000

- Yankee Group estimates \$5.6Billion market by year 2000 (4 years)

Source: Infosecurity product news, Yankee Group

9

Costs *(cont)*

- For Electronic Commerce to succeed the cost-of-entry into a secure environment has to be lower than 2% of per-transaction cost
 - More than fractions of a penny/transaction will be hard to justify
 - Many E-Commerce models are based on pennies per transaction profit margins

10

The Cost Problem

- For infrastructure providers (banks, E-banks, credit bureaus) that make their money on pennies per transaction, ***we need to make security 2 orders of magnitude cheaper***
- There is a huge disconnect between the high risk and low risk expenditures and potential exposure

11

Known Losses

- CSI Member Survey:
 - 30 respondents total over \$66million in losses due to infosecurity problems and cleanup
 - 2 respondents report losses over \$1million due to insider eavesdropping
- Average loss per incident is approximately \$80,000 to \$100,000

Source: Computer Security Institute

12

Known Losses (cont)

- GAO report Rome Air Force base security incident and cleanup costs \$211,700 not counting other agencies
- Citicorp security incident in Sept 1995 \$12million transferred illegally but **only** \$400,000 is lost and not recovered

13

Leverage

- Is ~\$201,000/year spent on infosecurity products justified against the losses that are being recorded?
- Does it show that security products provide adequate leverage?
 - I pay \$2,000/year auto insurance against \$300,000 liability with an estimated per-incident loss of \$2,000 to \$25,000

14

Cost (cont)

- Conclusion:
 - I think we're improving but security is not going to be attractive until costs lower by 2 orders of magnitude
- Corollary:
 - The small players will ignore security
- Observation:
 - Nobody has a handle on this problem

15

The Present

- Expenditures on infosecurity products:

22%	Don't know	
17%	Less than \$20,000	
12%	\$20,000 to \$49,000	
9%	\$50,000 to \$99,000	← (average cost/incident)
14%	\$100,000 to \$249,000	
9%	\$250,000 to \$499,000	
17%	\$500,000+	

Source: CSI

Source: Infosecurity product news

16

The Future: Predictions

- To get smaller players on board security product costs will continue to drop
 - By Q4 1996: \$200 secure web servers
 - By Q3 1997: \$400 firewalls
 - By Q1 1998: “free” security in routers, hubs, switches
- *Market growth will dilute quality of products: lack of expertise in security*

17

The Future: Predictions

- Security is now a product feature
- Within 2 years security will be like “low fat” cooking
 - Products that are laden with grease will be labelled as “lite” (Windows NT C2)
 - Products that have nothing to do with fat will be labelled as “fat free” (Secure UPS’)
- Nothing will improve

18

How do we Break the Cycle?

- We can either train s/w engineers to write security into V1.0 (which is expensive and they don't listen very well)

or

- We can continue to have to retrofit and patch and kludge around security flaws to fix V2.0 (same caveat as above)

19

Breaking the Cycle

- High quality support libraries are necessary as basic building blocks for secure applications
- We need the equivalent of secure `stdio.h`
- Build it into infrastructure so we don't have to rely on application developers to get it right

20

Breaking the Cycle (cont)

- Building security into infrastructure will require commitment from
 - Vendors
 - End users
 - Standards committees

**We're doomed,
aren't we?**

21

Core Issues

- These are the issues that will dominate future of Internet Security: (in no particular order)
 - Encryption
 - Executable Content
 - Firewalls
 - Electronic Commerce
 - User Communities
 - Software Development / Distribution

22

Encryption

23

Encryption: Today

- Reasonably usable crypto-APIs exist
- Reasonably usable crypto code exists
- Some applications use crypto: a minority
- Many applications that should use crypto do not because of:
 - Ignorance
 - Customer misperception of risk

24

Encryption: Today (cont)

- The single largest factors delaying the useful deployment of crypto:
 - Patents and intellectual property restrictions
 - Lack of leadership from standards bodies (vendor lobbyists)
 - Government intervention (export control)
- This is not a *technical* problem

25

Encryption: Tomorrow

- Export control regs will be gone by 2000AD
 - 80% likely: US businesses will lose to non-regulated foreigners
 - 18% likely: Washington will wise up
 - 2% likely: Government “software clipper” technology will be adopted
- By 2001AD we’ll see encryption all over

26

Encryption: Getting to the Future

- We need:
 - Reduced regulation
 - Increased packagability
 - Embedded in APIs (e.g.: Winsock, AWT, Java)
 - Embedded key management
 - Embedded in application development tools
 - Relevant and timely standards
 - No vendor lobbyists / competitive lock out
 - No more representational standards bodies

27

Executable Content

28

Executable Content: Today

- Java
 - Actually not too bad!
- ActiveX
 - Generic OLE capability
 - “click here to reformat your hard disk”
- PointCast
 - Downloads new versions automatically
 - Potential global virus broadcast system

29

Executable Content: Today *(cont)*

- Scary trends:
 - Increasingly easy to download and install anonymous plug-ins from random places
 - Increasing number of services overload on top of HTML (PointCast and others)
 - Tunnel through firewall
 - Indistinguishable from “legitimate” Web traffic
 - Viral macros (Word Concept) are machine-independent

30

Executable Content: Tomorrow

- It's going to be ugly

31

Firewalls

32

Firewalls: Today

- Rapidly growing market
 - Over 150 firewall products on market
 - Commoditization is around the corner
 - Vendors looking for ways to distinguish their offerings
 - Terminology
 - Market share
 - “Most-completest” security solution syndrome

33

Firewalls: Today *(cont)*

- Biggest problems today with firewalls:
 - Downloadable content
 - Performance concerns *(usually misplaced)*
 - Remote management
 - Ignorance: knowing what policies make sense within a firewall
 - What to allow in and how
 - What to allow out and when

34

Firewalls versus Host Security

- Many see a choice between firewalls (network level security) or host security
- Downloadable content is blurring the lines very rapidly

That's not an
"OR" question!

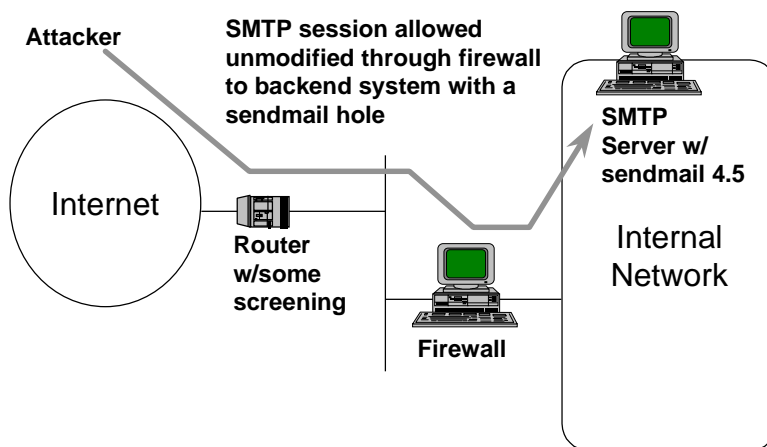
35

The Incoming Traffic Problem

- Data streams that are allowed in may not be protected or *protectable*
- Some firewalls perform application specific security on data streams
 - Others do not
 - Sometimes you can't - PGP+MIME
- Splits security between firewall and system on backend

36

The Incoming Problem (cont)



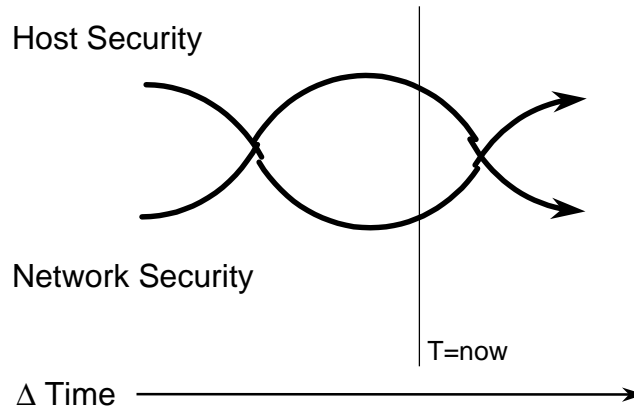
37

Incoming Traffic: Implications

- Security must be split between firewall and backend system to be effective
 - Host security raises its head - again!
 - Many admins do not realize they still need to worry: “we have a firewall so everything is OK now.”
- Sometimes the service is necessary w/no security: TN3270 to mainframe

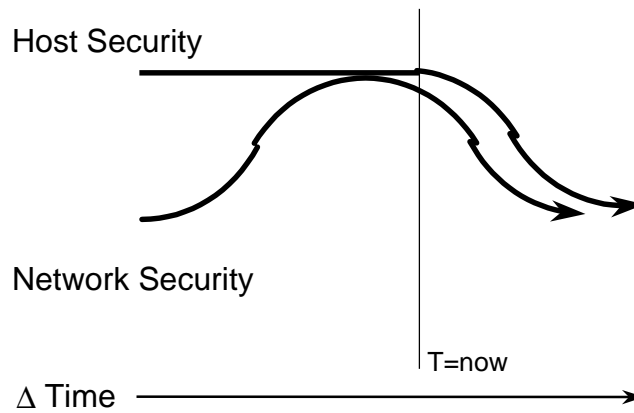
38

The Wish and Wash



39

Wish and Wash: Worst Case



40

Firewalls: Tomorrow

- Mixtures of firewalls and secure applications will co-exist
 - Based on bandwidth needs
 - Based on application requirements
- Firewalls will become a commodity
- Distinction between firewall types will primarily be marketing terminology
- Desktop security will still be terrible

41

Electronic Commerce

42

Electronic Commerce: Today

- Still embryonic
- Web-based GUI on top of federal express and credit card system
- **Real** electronic commerce will depend on useable electronic cash
 - Transmission of value
 - Transfer of funds

43

Electronic Commerce: Today

- Big problems to solve
 - Repudiation or revocation of a transaction
 - Credit cards do this badly, slowly, awkwardly
 - What about a **stock sale**?
 - Portable Identity
 - Authenticated user-identity that goes with you
 - Portable digital certificate
 - Smart cards likely crucial technology

44

Electronic Commerce: Tomorrow

- One scary thing to consider
 - To implement full-blown electronic commerce we'll need full-blown electronic cash
 - Ecash may be subject to same pressures as real cash
 - Deflation / Inflation
 - Currency trading
 - Devaluation

45

Electronic Commerce: Tomorrow

- Security is going to play a critical role for Electronic Commerce
- So far we've been doing a terrible job
 - Lack of standards
 - Gaping holes
 - Poorly designed systems
- We need to do better or we'll lose

46

User Communities

47

Managing User Communities

- What is needed are tools that organizations can use to manage customer E-commerce relations
 - Authentication
 - Integrity
 - Privacy
 - Non-repudiation
 - Eventually, delegation of trust

48

User Communities: Today

- Very primitive systems based on service provider-oriented access
 - CompuServe has online banking interface
 - AOL has online trading
 - etc.
- Initial attempts to migrate to Internet from closed systems have begun

49

User Communities: Today *(cont)*

- The battle for the future is being fought today over who controls the concept of *registered user*
 - Deliberate standards-fragmentation over certification hierarchies
 - Deliberate standards-fragmentation between E-cash and credit card alliances

50

User Communities: Digital Certificates

- Public key is an attractive technology
 - Makes the process of key management a lot simpler
 - Sounds extremely sexy

51

User Communities: Digital Certificates *(cont)*

- Public key does not address:
 - Can you trust issuer of certificate?
 - What is the certificate holder authorized to do?
 - Management of stolen certificates (yet)

52

User Communities: Digital Certificates (cont)

- Current model is based on credit card transaction model
- Other data needs to be stored someplace
- The transaction model may not apply
- *Every big bank on the planet is looking at digital certificates and waiting for the technology to stage a break-through*

53

User Communities: Smart Cards

- Smart cards are a *key* technology in the future
 - Certificates are “large” and need to be stored someplace
 - How many of you want to memorize and type in a 1024-bit RSA key?
- Stored value cards are coming

54

User Communities: Smart Cards (cont)

- Current model is based on credit card transaction model
- Data storage on card represents great integration opportunity
- *Every big bank on the planet is looking at smart cards and waiting for the technology to stage a break-through*

55

Delegation of Trust

- Ecommerce will become truly interesting when delegation of trust occurs
- Corporations cross-accepting eachother's digital certificates and stored value smart cards
- Growth model is very familiar

56

Delegation of Trust *(cont)*

- Phase 1: ATM cards
 - Each bank has own machines
 - Customers not used to technology
 - Nobody sure it will be a success
- Phase 2: Local acceptance
 - Local banks begin to permit “foreign” cards
 - Customers can now use card within metropolitan area

57

Delegation of Trust *(cont)*

- Phase 3: Delegation of trust
 - Ubiquity achieved
 - Consortia (MOST, etc) cross accept all members' cards
 - Cards now usable world-wide (mjr gets cash in Tokyo with card issued in Baltimore, MD)

58

Software Development

59

Software Development: Today

- Amazingly vigorous and profitable industry
- US leads hands-down in innovation
- We're also almost completely clueless about security in our development practices

60

Software Development: Today

- Any idiot with a compiler could write the next “killer app” that will be driving your business next year

61

Software Development: Today

- Big Problems:
 - Code quality (from a security perspective)
 - Code trustworthiness (who wrote it anyhow?)
 - Code distribution (is what you’re running what the vendor really wrote?)

62

Code Quality

- How do we build secure systems when the people writing 99% of the code in the world know nothing about security?
- How can we fix all the broken code which is being churned out?
- This problem grows more acute every day

63

Code Trustworthiness

- The ultimate hacker's paradise: get a job at Microsoft and work on the NT sources
- How can we establish any degree of confidence in security of development practices?
 - background checks?
 - code reviews?

64

Code Distribution

- With a \$500 CDROM burner and a \$4,000 CDROM printer I can make a disk that looks just like an NT SDK update and send it to my victim
- Increasing number of patch downloads over Web
- No integrity signature or check on most downloads

65

Where are we now?

66

1997: Security Environment

- Firewalls
 - Boundary access control
- Encryption
 - Data integrity and confidentiality
- Digital Signatures
 - Electronic identity
 - May be used for authentication
 - Backbone for E-commerce (*maybe*)

67

1997: Security Environment (cont)

- Dialup Networking
 - Mostly insecure
 - Must rely on other (external) security, e.g.:
firewalls and encryption
- The Web
 - Server side security
 - Client side security

68

1997: Main Problems

- Client-side execution
 - Java, ActiveX, Pointcast plugins
 - Poor security model weakens desktop
- Server-side execution
 - “Secure” web servers use a secure *protocol* to talk to an insecure *service*
 - Most CGI developers are “security challenged”

69

1997: Main Problems *(cont)*

- Business perception
 - Internet risks are distorted
 - Some see Internet as no risk (and shouldn't)
 - Some see Internet as huge risk (and shouldn't)
 - Relatively few organizations understand their security exposure or countermeasures

70

1997: Main Problems *(cont)*

- Government intervention
 - Law enforcement is useless on the 'net
 - Legislation is useless on the 'net
 - Restrictions on use of encryption are increasing
 - Attempts at regulating E-commerce are being considered (with likely disastrous or laughable results)

71

1997: Main Problems *(cont)*

- Trust boundaries
 - Nobody really knows who they are connected to anymore
 - Many organizations are connected to their competitors and don't know it

72

What's Hot: Firewalls

- Firewalls now a commodity technology
 - Differences between “turbo-whomping adaptive psychic packet filter” and “application gateway” are increasingly blurred
 - *Most important factor in firewall's configuration is how the end user installs it*

73

What's Hot: Encryption

- Little progress in this area

74

What's Hot: Digital Signatures

- X.509 is becoming standard
 - Encodings of X.509 certificates are not :(
- Widespread use will prompt widespread theft starting soon
 - Smart card storage is next step
- Too many certificate issuers
 - Whose certificate can you trust?
 - Nobody's?

75

What's Hot: Dialup Networking

- Dialup networking still a game of Russian Roulette
 - Presently no vendors supporting built-in encryption dialup TCP/IP
 - Very few support CHAP authentication
 - Most rely on passwords
 - Some desktops may route traffic
- Lots of work to do in this area

76

What's Hot: The Web Server

- Hackers altering web pages
 - So put it on a Jaz disk!!!!
- Server side encryption is OK
 - Remaining problems of how to get transactions in through firewalls
 - What about attacks against CGI scripts that are launched over secure channels?

77

What's Hot: The Web Client

- This changes too fast to contemplate
- Bad news:
 - More plugins
 - More client side code
 - More security holes
 - Constant flow of “new standards” makes it impossible to fix the broken stuff
 - Disaster looms

78

Summary

- Lots of work is being done in security
- The problems are being attacked piecemeal (perhaps that's the *only* way to attack them!)
- Lack of standards and unification increases exposure to bugs and flaws
- Life will continue to be ***interesting***

79

Conclusion

80

May you live in interesting times

81

The Future?

- This talk has been about the future
- Can we believe that things really will get better?
- Or will we do more of the same faster and just as badly as before?

82

An Analogy

- Cars begin appearing on the market in 1890's-1900's
- By 1920's cars capable of speeds in excess of 60mph
- It must have been ***accepted as a matter of course*** that when you had an accident you ate the dashboard
- Seatbelts appear in 1950's

83

Analogy (cont)

- Window of 60 years between introduction of passenger safety technology into a known dangerous product
- Industry resistance and consumer resistance continues to this day
- ***We are in the padded dashboard phase of network security***

84

Questions?

- Questions?
- Comments?
- Tomatoes?