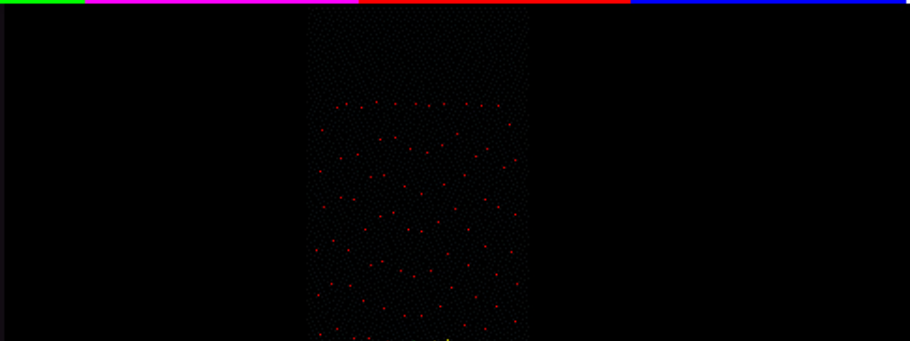


Systems Security



Cryptographic Protocols

n Key Exchange



Asymmetric-Key Exchange

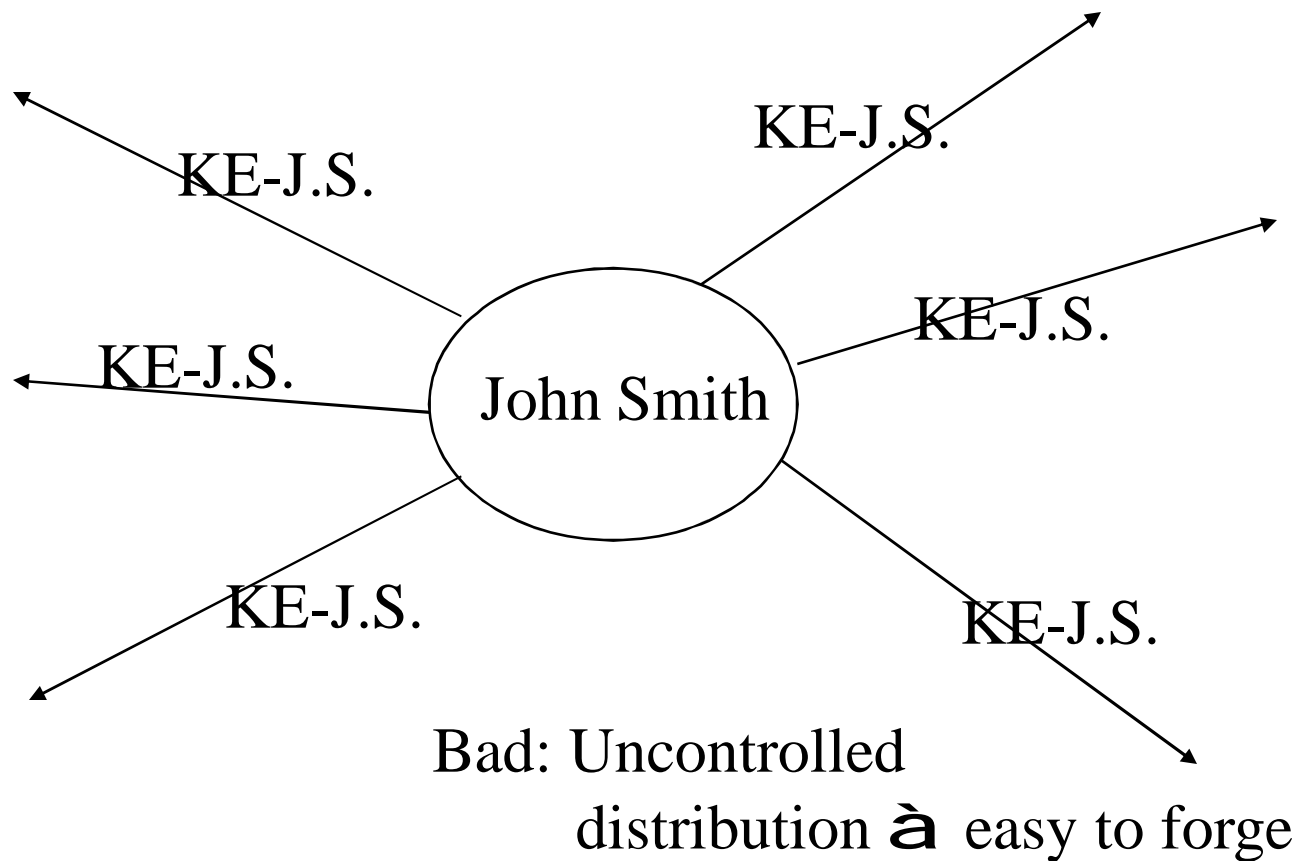
n Without server

- .. Broadcasting
- .. Publicly available directory

n With server

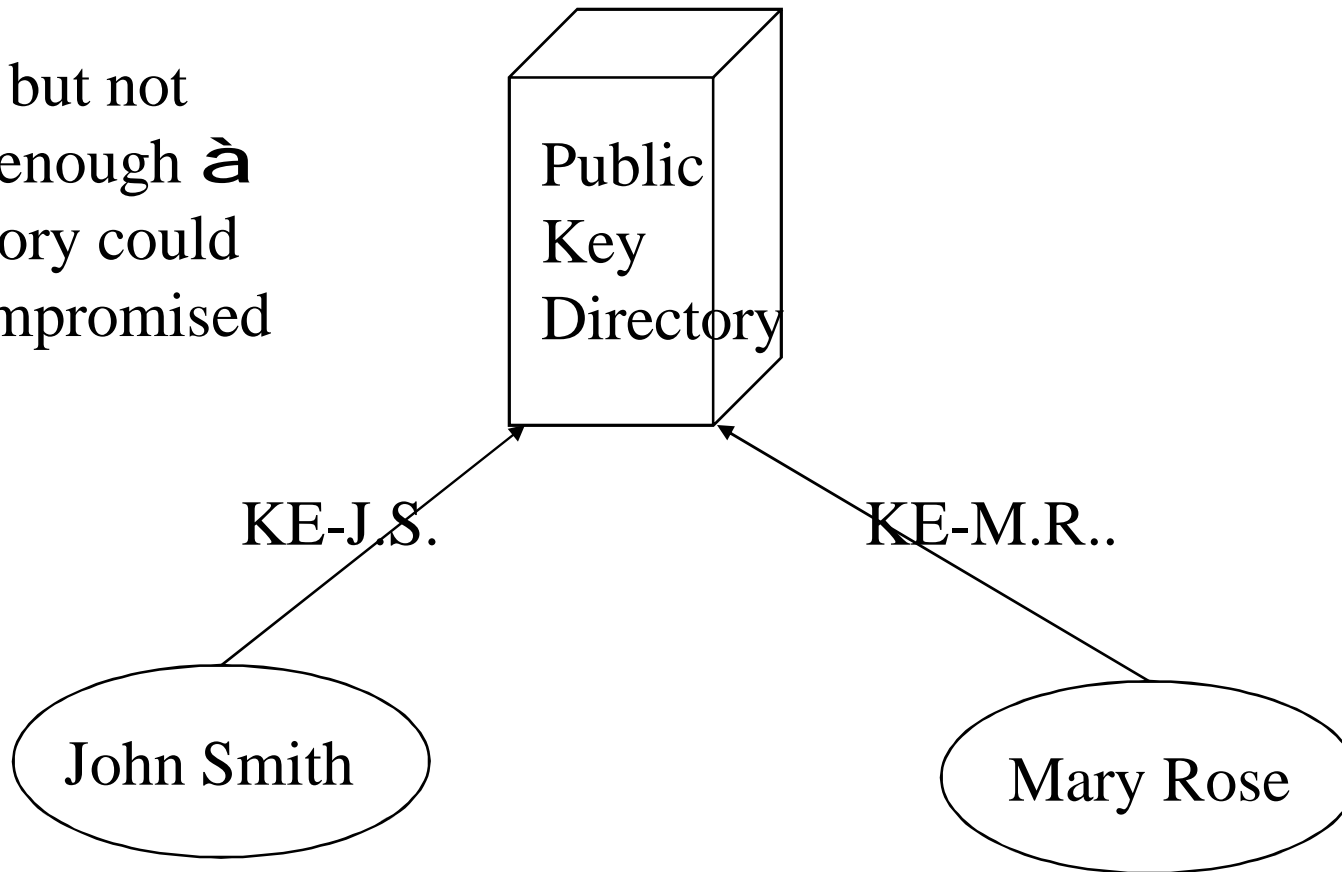
- .. Public key distribution center
- .. Certificates

Public announcement

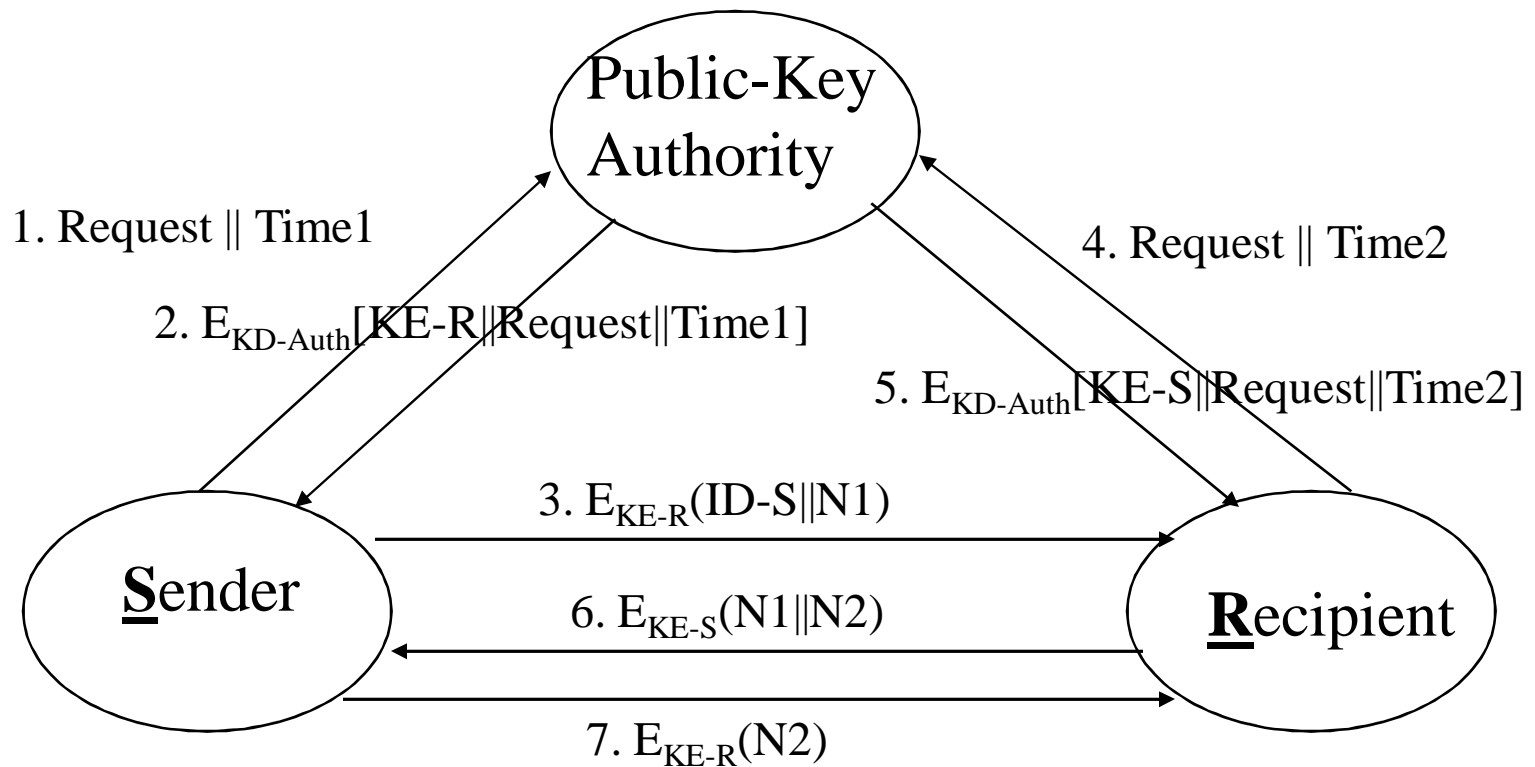


Publicly available directory

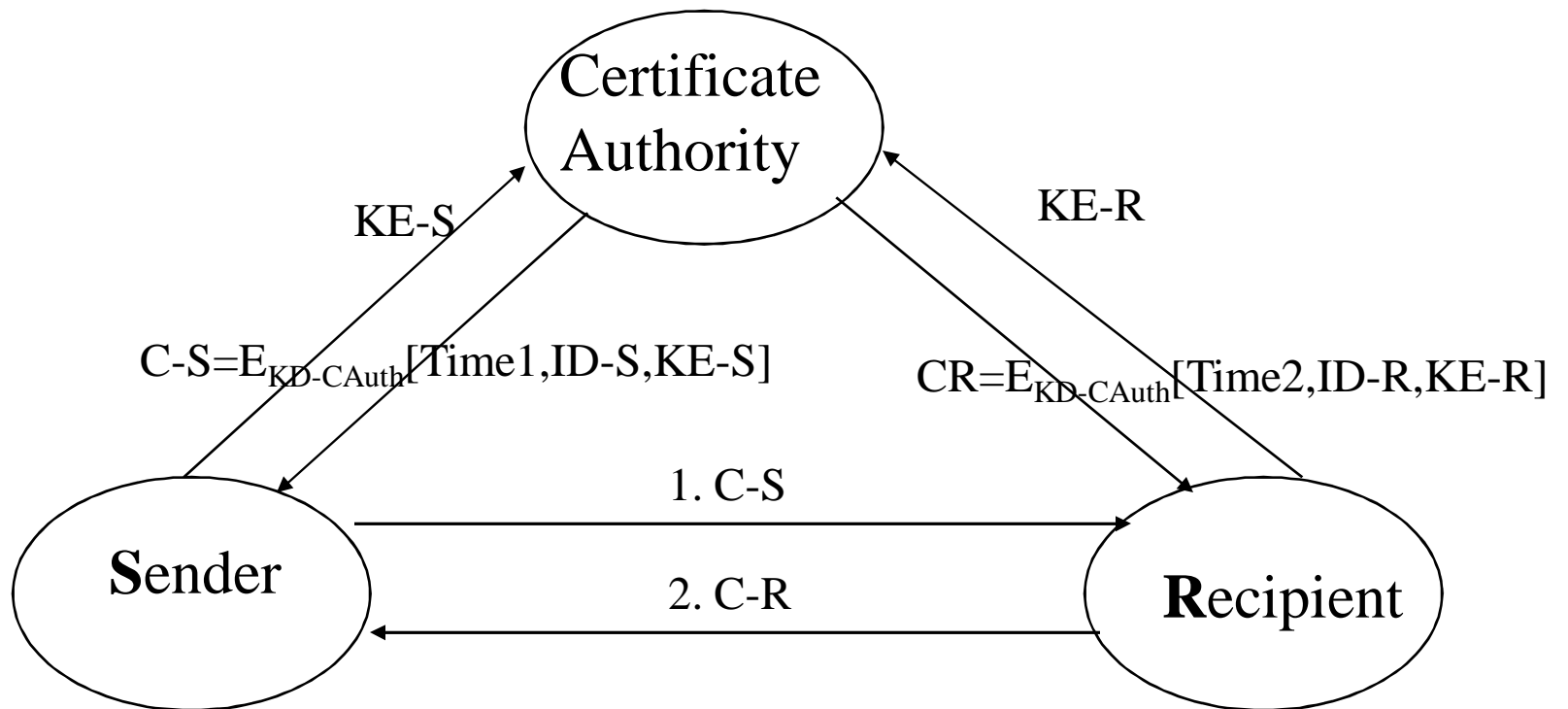
Better but not
Good enough à
Directory could
Be compromised



Public-key authority



Public-key certificates





Certificates

- n Guarantees the validity of the information
- n Establishing trust
- n Public key and user identity are bound together, then signed by someone trusted
- n Need: digital signature



Digital Signature

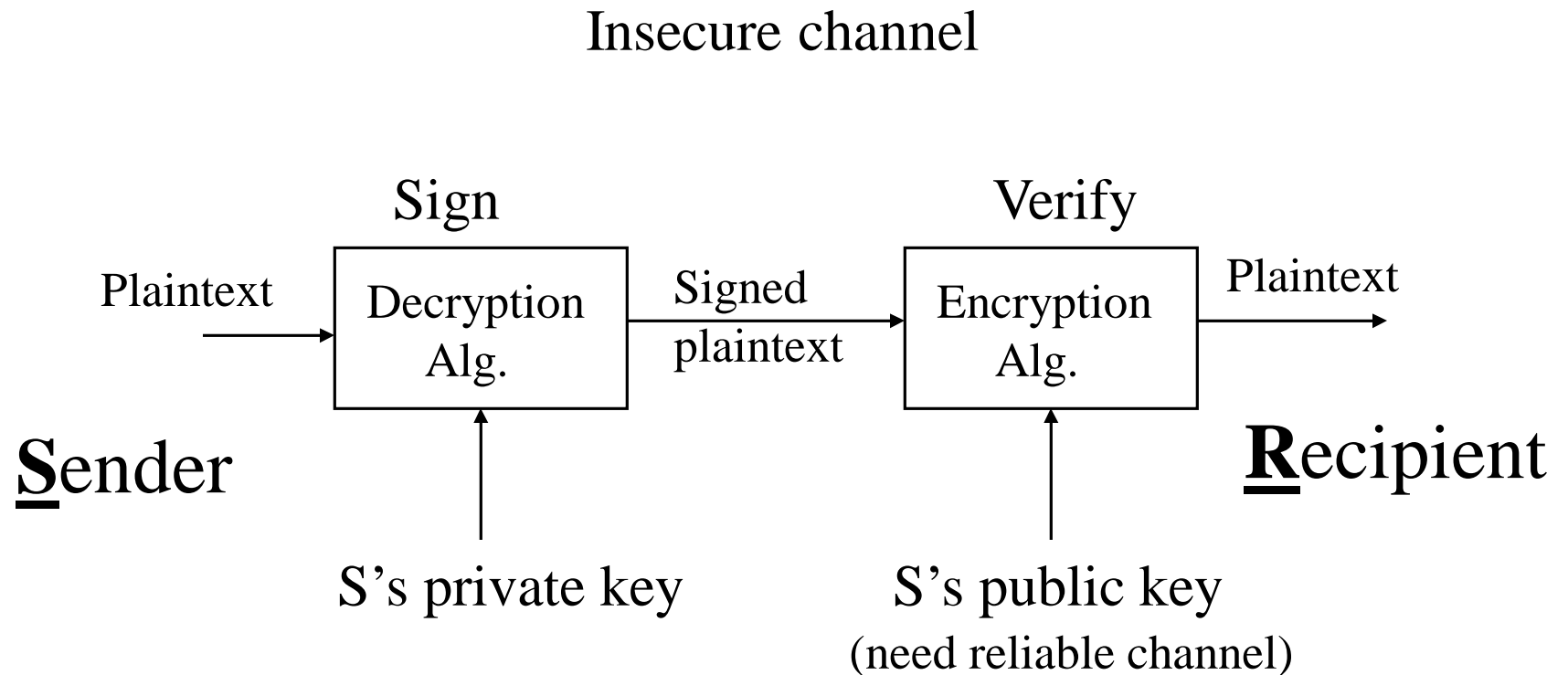
- n Need the same effect as a real signature
 - .. Un-forgable
 - .. Authentic
 - .. Non-alterable
 - .. Not reusable



Digital signature

- n Direct digital signature: public-key cryptography based
- n Arbitrated digital signature:
 - .. Conventional encryption:
 - n Arbiter sees message
 - n Arbiter does not see message
 - .. Public-key based
 - n Arbiter does not see message

Digital Signatures in RSA





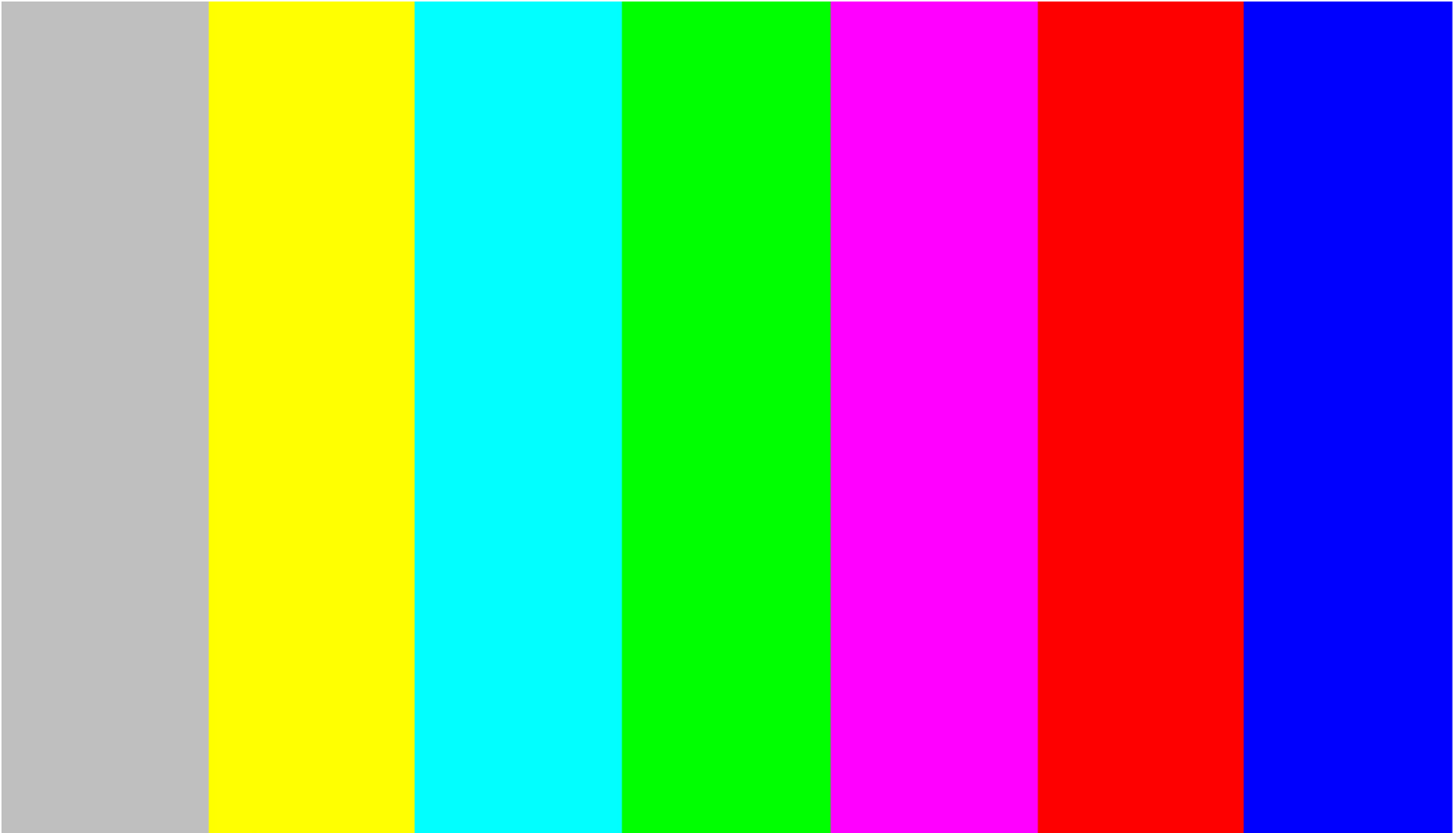
Non-repudiation

- n Requires notarized signature, involving a third party
- n Large system: hierarchies of notarization

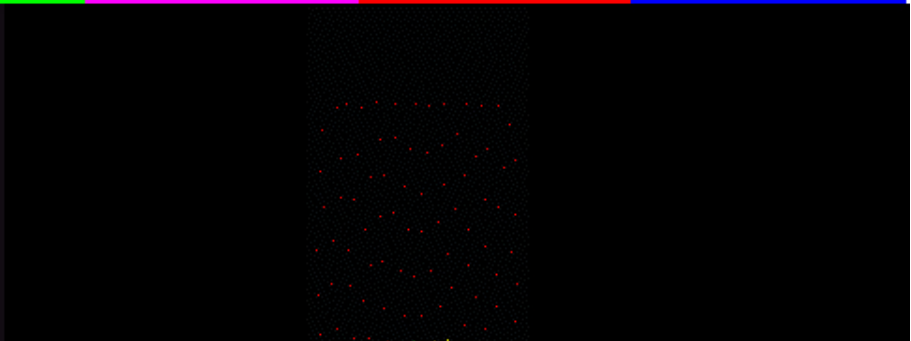
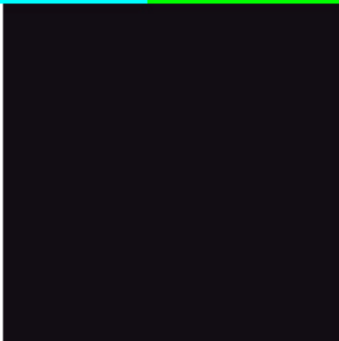


Voting System

- n **Goal:** to establish the intent of the voter, and transfer that intent to the vote counter
- n **Assumptions:**
 - .. Vote is open and everyone can monitor it
- n **Requirements:**
 - .. Anonymous
 - .. Scalable (speed, efficiency)
 - .. Auditable
 - .. Accurate
- n **Need to focus on accuracy and availability**



Systems Security





Personal Security and Privacy on the Web



J. Edgar Hoover:

- n "Why should you care if you have nothing to hide?"



'There are worse things
than having your privacy
violated ... like murder.'



Privacy

"Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men."

Ayn Rand, *The Fountainhead* (1943)

<http://www.aynrand.org/>



Loss of Privacy

- n “Consumer Relationship Management” \$40 billion in 2000, \$90 billion by 2003
- n Acxiom keeps personal and lifestyle data on 95% of U.S. households and can arrange it according to ethnicity, race or other criteria



Loss of Privacy

- n Web sites unknowingly send data to advertisers, June 14, 2000
- n E-sign bill passed by the House in a 426-4 vote. June 14,2000
- n “Safe Harbor” US-EU agreement offers more than American companies offer customers at home. June 12, 2000




Loss of Privacy

- n New breed of viruses: Caligula sends data over Internet. Feb 1999.
- n Accidental Release of Info: University of Michigan Health System, 18 MB of patient's data; Feb 1999




Loss of Privacy

- n FTC surveyed 1400 web sites: 92% collect personal info; only 14% notify users; only 2% have a privacy policy; June 1998
- n Example: www.engage.com has garnered 30 million user profiles; Aug 1998.




Your Privacy and Security is Compromised ...

- n When you e-mail
- n when you surf the Web
- n when you have a home page



Your Privacy and Security is Compromised ...

- n When your PC is on-line
- n When your PC is idle ...



CommerceNet/Nielsen survey on Internet Usage (Spring 1999)

- n 92.2 million Americans over age 16
- n an increase of 14 million from the 1998



Connecting to the Net

- n NIC: Ethernet Card Address
- n Modem + PPP
- n You are a node on the Net
- n IP address



Network Security Breaches

- n All the usual breaches; in particular:
- n A program runs on your machine without your permission
- n You are impersonated



Firewalls provide ...

- n Filtering of network packets to/from certain addresses and ports.
- n Detailed logs of who accessed what, when, and for how long.



Firewalls do not provide ...

- n Security of personal data
- n Authentication of Individuals
- n Anonymity
- n Alerts when an unauthorized program runs



Globally Unique Identifiers

- n Each document created by Word, ... has a guid.
- n Windows install generates a guid.
- n Registration sends this and other info.



Pentium III

- n “designed with the Internet in mind”
- n The PSN (processor serial number) is built into the silicon chip during manufacturing



Intel Assures ...

- n the serial number can be turned off with a utility
- n to develop tools and guidelines on the responsible use of the processor serial number.
- n it will not maintain a database that correlates processor serial numbers with consumers



Fact Is ...

- n the serial number can be turned on with a remote utility (ActiveX, ...)



Processor Serial Number

- n Intel has not removed the PSN from its P3.
- n Intel admitted that some Pentium II chips contain the PSN.
- n Intel will not include a PSN in its upcoming chip.



Give yourself privacy in electronic communications

n Understand the scientific basis for privacy:

Cryptography.



Security of Content

- No observer can read the contents of the message
- n No observer can identify the sender and receiver



Integrity of Message

- the message has not changed
- the message has not been prevented from reaching the recipient



Sender and Receiver

- n Only the intended recipient receives the message
- n The message is sent by the claimed sender
 - The sender cannot deny
 - The recipient cannot deny



www.EPIC.org

Guide to Practical Privacy Tools

- § Snoop Proof Email
- § Anonymous Remailers
- § Surf Anonymously
- § HTML Filters
- § Cookie Busters
- § Voice Privacy
- § Email and File Privacy
- § Encryption
- § Disk/File Erasing Programs
- § PC Firewalls



PGP

- n “Pretty Good Privacy”
- n Uses two coupled keys: Public key published; Private key kept secret
- n Plug-ins for many e-mail packages
- n File storage applications also



Anonymizers

- n Everything *you* do on the Web can be attributed to *you*.
- n Anonymizer.com “Privacy is your right”
- n Search on “anonymous remailers”



SSL

- n “Secure Sockets Layer” 2.0 3.0
- n Transport layer
- n authenticated: servers, always; clients, optionally
- n uses encryption



HTTPS

- n Secure HTTP
- n application protocol
- n Client/Server Authentication
- n Spontaneous Encryption
- n Request/Response Non-repudiation



Privacy Checklist

- Minimize the information that you put in your mail signature files.
- Reconsider what you have in your personal web pages.
- Consider what information you give out to web sites.



Privacy Checklist

- Search the people locators to find out what sites list your personal information.
- Have yourself removed from spam mailing lists.
- Your posts on a newsgroup or mailing list can imply a great deal about you.



Privacy Checklist

- Frequently delete your browser's history and cache files.
- Understand cookies.
- Use PGP.



Privacy Checklist

- n Do not use “What’s Related?”
- n Do not use “Show Related Links”
- n Apply MS Office patches to remove GUID feature.
- n Remove GUIDs from existing documents.



Cookies

- n A text file on your HDD that a browser creates at the request of a web site
- n Can contain arbitrary data
- n Not meaningfully editable by you (?!)

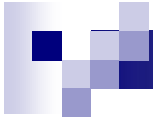


MRU, ...

- n “Most Recently Used” items
- n TweakUI from MS
- n more properties, www.imaginary.co.za
- n www.xteq.com



TweakUI



MoreProperties




If you want privacy in the electronic age ...

- n You have to give it to yourself.
- n Your employer will not give it to you.
- n Your government will not give it to you.
- n Even the laws of your nation cannot be relied upon to give it to you.



Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.



Art 12: Universal Declaration of Human Rights

- n “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”



Loss of Privacy

"You already have zero privacy -- get over it."

Scott McNealy, 1999, Sun



Get Over It?

"First they came for the hackers.
But I never did anything illegal with my computer,
so I didn't speak up.
Then they came for the pornographers.
But I thought there was too much smut on the Internet anyway,
so I didn't speak up.
Then they came for the anonymous remailers.
But a lot of nasty stuff gets sent from anon. penet. fi ,
so I didn't speak up.
Then they came for the encryption users.
But I could never figure out how to work PGP anyway,
so I didn't speak up.
Then they came for me.
And by that time there was no one left to speak up."

-- Unknown



FBI

is asking Congress for the right to view the encrypted computer files of consumers, ... -- without the owner's knowledge.



ACLU: Privacy Principles

- n Your personal information should never be collected or disseminated without your knowledge and permission.
- n Organizations must let you know *why* they're collecting your information; and they can't use it for other reasons than the one you granted permission for (unless they get a second permission from you)



ACLU: Privacy Principles

- n Organizations must ensure the privacy of the personal information they collect or maintain on you, retaining only what is necessary information and only for as long as it is needed.
- n You should have the right to examine, copy, and correct your own personal information.



ACLU: Privacy Principles

- n There must be no national ID system -- either in law or in practice
- n Unrelated data bases must be kept strictly separate so information can't be cross-referenced.
- n Personal "biometric" data -- your fingerprints, DNA, retina or iris scans, etc. -- must not be involuntarily captured or used (except for fingerprinting criminals).



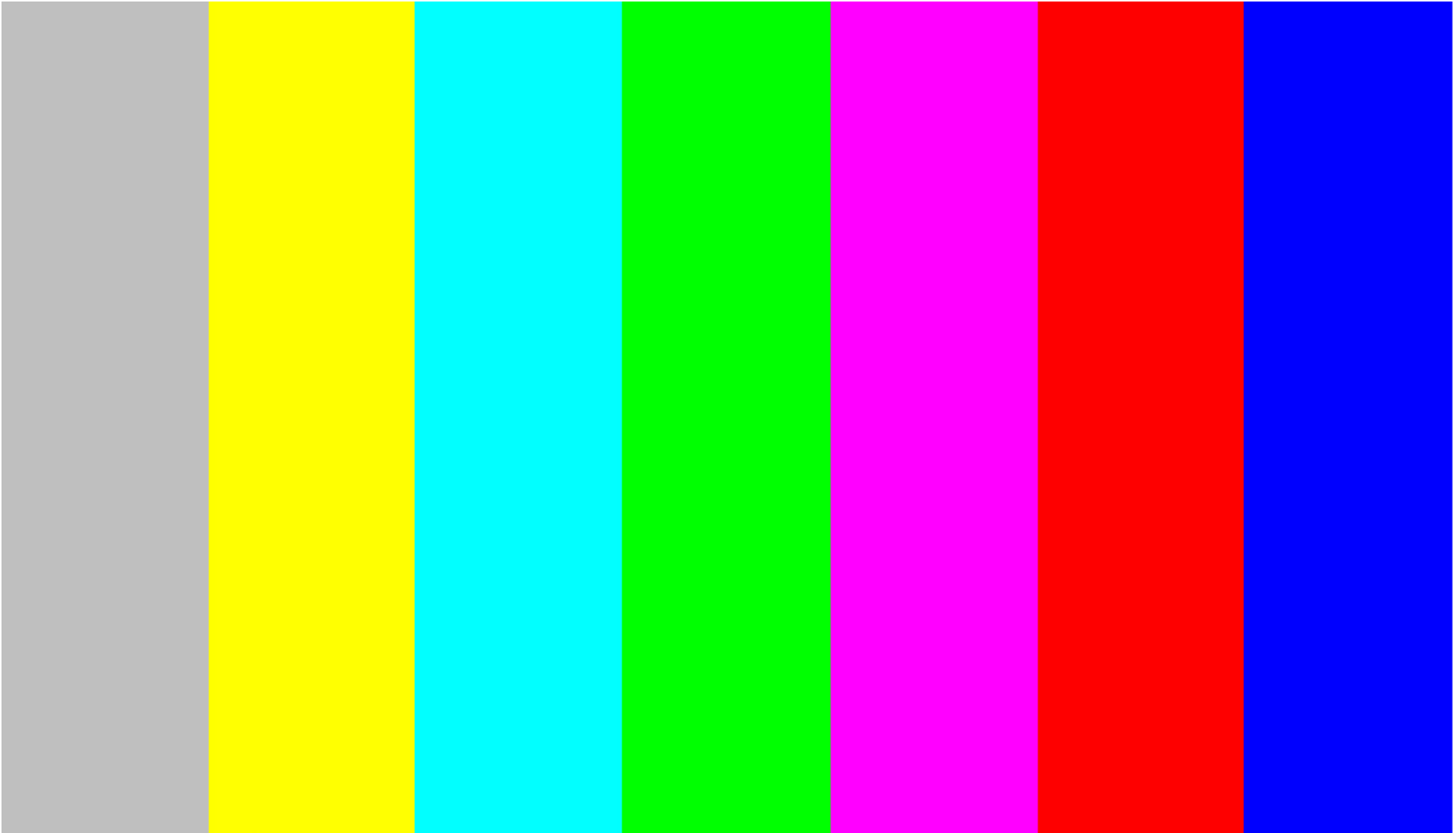
ACLU: Privacy Principles

- n The government must not prohibit or interfere with the development of technologies that protect privacy (such as encryption).
- n These principles should be enforceable by law. Furthermore, no service, benefit, or transaction should be conditioned on waiving your privacy rights.



Get Over It?

- n Write your local elected officials and tell them you want stronger laws to **protect your privacy.**
- n **"Cyberspace must be free!"**
- n <http://aclu.org/>



Systems Security

