Miscellaneous Topics

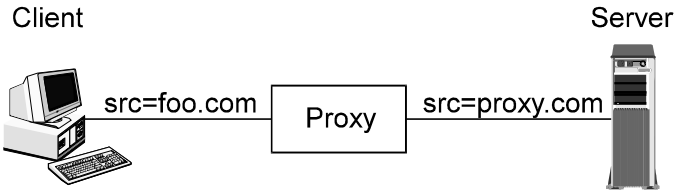
Buy a rifle, encrypt your data, and wait for the revolution

Traffic Analysis

Monitors presence of communications and source/destination

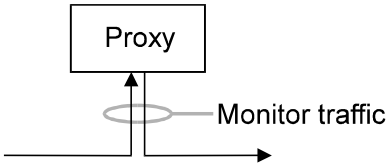
- Most common is analysis of web server logs
- Search engines reveal information on popularity of pages
- The mere presence of communications can reveal information

Simple Anonymiser Proxy



HTTP version at `http://www.anonymizer.com`

Fairly easy to defeat:

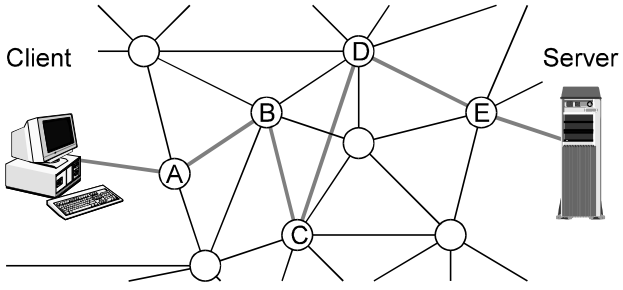


Mixes

Encrypted messages sent over a user-selected route through a network

- Packet = A(B(C(D(E(data)))))
- Each server peels off a layer and forwards the data

Servers can only see one hop



Sender and receiver can't be (easily) linked

Attacks on Mixes

Incoming messages result in outgoing messages

- Reorder messages
- Delay messages

Message sizes change in a predictable manner

Replay a message (spam attack)

- Many identical messages will emerge at some point

Onion Routing

Message routing using mixes

Routers have permanent socket connections

Data is sent over ephemeral connections tunnelled over permanent connections

- 5-layer onions
- 48-byte datagrams
- CREATE/DESTROY for connection control
- DATA/PADDING for datagrams
- Limited form of datagram reordering
- Onions are padded to compensate for removed layers

Mixmaster

Uses message ID's to stop replay attacks

Message sizes never change

- 'Used' headers are moved to the end, remaining headers are moved up one
- Payload is padded to a fixed size
- Large payloads are broken up into multiple messages
- All parts of the message are encrypted

Message has 20 headers of 512 bytes and a 10K body

Crowds

Mixes have two main problems

- Routers are a vulnerable attack point
- Requires static routing

Router vulnerability is solved via a jondo (anonymous persona)

Messages are forwarded to a random jondo

- Can't tell whether a message originates at a given jondo
- Message and reply follow the same path

Later updates took steps to hide the initiator

- Hordes uses multicast
- Herbivore (reaction to the FBI's Carnivore) uses broadcast

LPWA

Lucent Personalised Web Assistant

- Provides access to web sites via the LPWA proxy
- Automatically generates per-site pseudonymous personas
  - User name
  - Password
  - Email address
- Filters sensitive HTTP headers

LPWA (ctd)

Protects users from profile aggregation, spamming

- User connects to LPWA using an email address and password
- When a web site asks for identification information, the user types `\u` (user name), `\p` (password), `\@` (email address)
- Proxy translates these to per-site pseudonymous personas

Email forwarder forwards mail to the user's real email address

- Spam sources can be blocked on a per-persona basis

Anonymiser Redux

No-one knows who the attackers are, or whether they even exist

- People ascribe supernatural powers to attackers
- Lots of fun dreaming up countermeasures for threats that may or may not exist
- Much activity both in conference papers and software
- New software appears to counter hypothetical threats against existing software

Tor (The Onion Router)

Designed to be a pragmatic, practical implementation of an anonymiser implemented via onion routing

Original onion router was a rather fragile research prototype

- Critical design and deployment issues were never resolved
- Tried to combine anonymity and protocol cleaning (to avoid fingerprinting)
  - Required separate application proxies for each protocol
  - Few were ever written

Tor (The Onion Router) (ctd)

- Traffic shaping (batching, reordering packets) was problematic
  - Later research (and experience) showed that it wasn't practical, economical, or even very useful against attackers
- Flooding-based state distribution didn't work
- Built a separate circuit for each application request
  - Requires multiple PKC operations for each request
  - Allowed fingerprinting based on the volume of circuits set up
- No integrity checking within a circuit
  - Packets were encrypted with a stream cipher
  - Malicious nodes could modify packets in transit
  - `ls` → `rm *`

Tor Design Principles

Must be usable in the real world

- Economical with bandwidth
- Easy to deploy
  - No kernel patches, some-assembly-required installation, …
- Easy to use
- Straightforward, easy-to-analyse design

Realistic threat model

- Strikes a balance between usability and security
- Fairly unique among crypto designs

Tor Design Details

Uses SOCKs as a universal interface

- Defers to the Privoxy privacy proxy for people who want protocol cleaning

Even with SOCKs, you have to be careful though

```
IP_addr = DNS( hostname );
connection = SOCKS( IP_addr );
```

- Can identify a client by linking DNS lookups and the final connection

Uses Tor nodes as directory servers to distribute state in batch mode

Tor Design Details (ctd)

Multiplexes multiple streams along each circuit

Checks packet integrity before it exits the circuit

- Per-hop MAC tags would expand the message at each hop
- Only the client knows all of the MAC keys

Provides for hidden servers within the Tor network

Takes steps to reassure volunteers running Tor nodes

- Rate-limiting controls bandwidth usage
- Exit policies allow control over addresses and ports that can be accessed from exit nodes
- Most nodes are configured as restricted exits that prevent access to abuse-prone services like SMTP

Tor General Operation

Routers maintain persistent TLS connections to other routers

- DHE key exchange signed with long-term router identity keys
- Identity key also signs directory updates

Establish an initial circuit to a Tor node

- Extend the circuit to new nodes as required
  - Circuits are identified by MPLS-style tags
  - Terminates at a chosen exit node
- Send data over the circuit in 512-byte packets

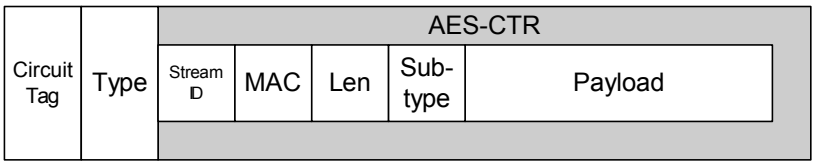
Multiple levels of multiplexing

- Circuits are multiplexed over a TLS connection
- Streams are multiplexed over a circuit

Tor Control Packets

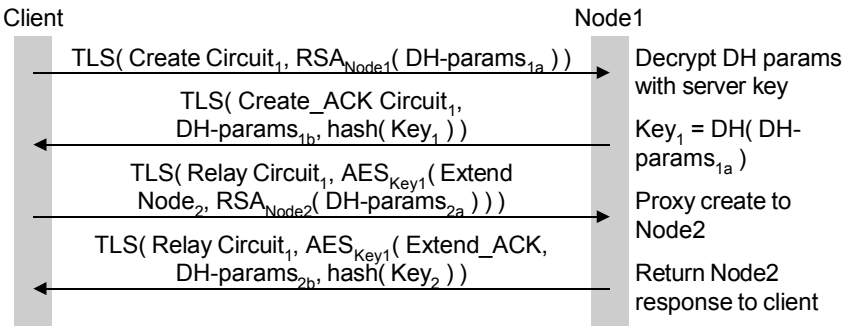
- Circuit tag is the MPLS label for the circuit
- Type is
  - Create / Create_ACK to establish a circuit
  - Relay to transport data along a circuit
  - Destroy to tear down a circuit
  - Padding used for keepalives

Tor Data Packets



- Circuit tag as for control packets
- Type = "Relay"
- Stream ID used for stream multiplexing within the circuit
- MAC is used for integrity checking by the exit node
- { Len, Subtype, Payload } contains the actual data
  - Encrypted/decrypted in AES-CTR mode by each node on the circuit

Tor Handshake



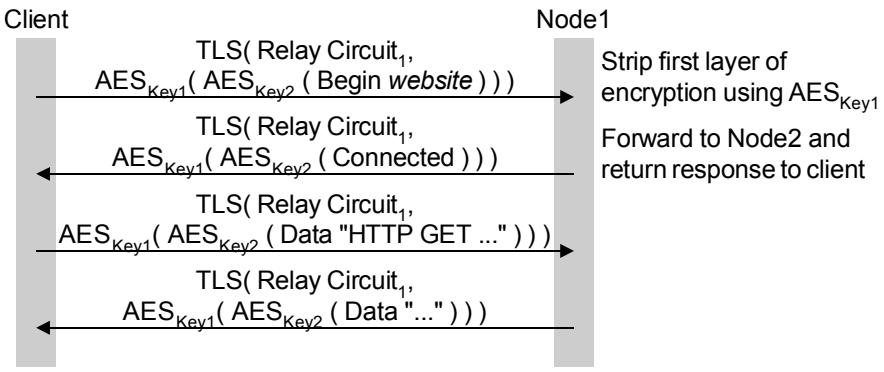
Circuit is extended one hop at a time

- At each extension, node *n* acts as a proxy for node *n*+1
- 'Relay Extend' at router *n* becomes 'Create' when proxed to router *n*+1

Tor Handshake (ctd)

Uses encryption to server rather than signing by client because a packet is too small for both DH parameters and a signature

Tor Data Exchange



Each node adds or removes a layer of encryption using the key it shares with the client as the message passes through

Tor Data Exchange (ctd)

Circuits are rebuilt periodically, typically once a minute

- Complicates traffic analysis
- Improves fault-tolerance

Once the final layer of encryption is removed, the packet exits the network

- Leaky pipe topology means a single circuit can have multiple exit nodes

Steganography

From the Greek for “hidden writing”, secures data by hiding rather than encryption

- Encryption is usually used as a first step before steganography

Encrypted data looks like white noise

Steganography hides this noise in other data

- By replacing existing noise
- By using it as a model to generate innocuous-looking data

Hiding Information in Noise

All data from analog sources contains noise

- Background noise
- Sampling/quantisation error
- Equipment/switching noise

Extract the natural noise and replace it with synthetic noise

- Replace the least significant bit(s)
- Spread-spectrum coding
- Various other modulation techniques

Examples of channels

- Digital images (JPEG, PhotoCD, GIF, PNG)
- Sound (WAV files)
- ISDN voice data

Generating Synthetic Data

Usually only has to fool automated scanners

- Needs to be good enough to get past their detection threshold

Two variants

- Use a statistical model of the target language to generate plausible-looking data
  - "Wants to apply more or right is better than this mechanism. Our only way is surrounded by radio station. When leaving. This mechanism is later years".
  - Works like a text compressor in reverse
  - Can be made arbrtrarily close to real text

Generating Synthetic Data (ctd)

- Use a grammatical model of actual text to build plausible-sounding data
  - "{Steganography|Stego} provides a {means|mechanism} for {hiding|encoding} {hidden|secret} {data|information} in {plain|open} {view|sight}".
  - More work than the statistical model method, but can provide a virtually undetectable channel
  - Infinite types of other embedding techniques are possible

Problems with steganography

- The better the steganography, the lower the bandwidth

Like anonymisers, mainly used as a source of conference papers

Watermarking

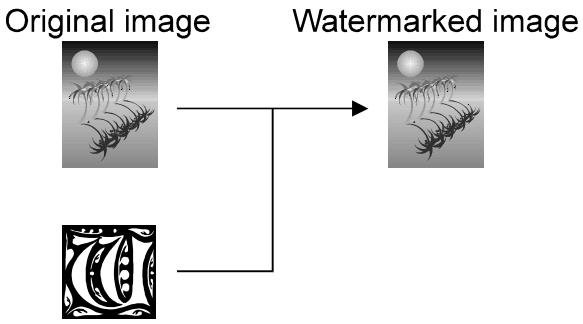
Use redundancy in an image/sound to encode information

Requirements

- Invisibility
- Little effect on compressability
- Robustness
- High detection reliability
- Security
- Inexpensive

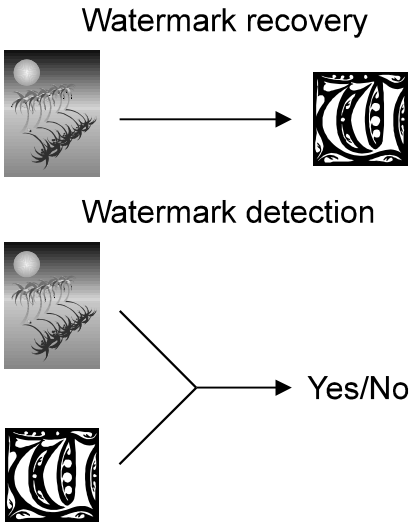
Watermarking (ctd)

Watermark insertion



Watermarking (ctd)

Watermark detection/checking



Watermarking (ctd)

Public watermarking

- Anyone can detect/view the watermark (and try to remove it)

Private watermarking

- Creator can demonstrate ownership using a secret key

Defeating Watermarking

Lossy compression (JPEG)

Resizing

Noise insertion (print+scan)

Cropping

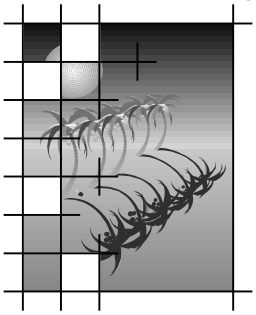
Interpretation attacks (neutralise ownership evidence)

Automated anti-watermarking software available (e.g. UnZign)

```
repeat until no watermark detected
    perturb content
    check for watermark presence
```

Defeating Watermarking (ctd)

Presentation attacks (segmented images)



Watermarking is still in its infancy

- No watermarking standards
- No indication of security/benchmarks
- No legal recognition

Other Crypto Applications

Hashcash

- Requires finding a collision for *n* bits of a hash function
  - "Find a message for which the last 16 bits of the SHA-1 hash are 1F23"
- Forces a program to expend a (configurable) amount of effort before access is granted to a system or service
- Useful for stopping denial-of-service attacks
  - *n* varies as the system load goes up or down
  - Can be used as a spam-blocker

Other Crypto Applications (ctd)

PGP Moose

- Signs all postings to moderated newsgroups
  - Signature is added to the message as an `X-Auth` header
- Unsigned messages (spam, forgeries) are automatically cancelled
- Has so far proven 100% effective in stopping newsgroup spam/forgeries

TEMPEST

Sometimes claimed to stand for Transient Electromagnetic Pulse Emission Standard

Known since the 1950's, but first publicised by van Eck in 1985

- Provided details on remote viewing of computer monitors
- Required about $15 worth of parts (for sync recovery)
- The spooks were not happy

TEMPEST Principles

Fast-rise pulses lead to harmonics radiated from semiconductor junctions

- Used to detect bugs
  - Flood the room with microwaves
  - Watch for radiated responses

Anything that carries a current acts as an antenna

TEMPEST monitoring gear receives and interprets this information

TEMPEST Sources

Computer monitor/laptop screen

- Generally radiates huge amounts of signal (range of hundreds of metres)
- Most signal is radiated to the sides, little to the front and back
- Requires external horizontal/vertical sync insertion, since sync frequencies are too low to be radiated
- Individual monitors can be picked out even when other similar monitors are in use
- Jamming is often ineffective for protection
  - Eavesdroppers can still zero in on a particular monitor

TEMPEST Sources (ctd)

Keyboard

- Some keyboards produce distinct RF signatures for each key pressed
- Active monitoring
  - Beam RF energy at the keyboard cable
  - Reflected signal is modulated by abscence/presence of electrical current

Ethernet

- UTP can be intercepted over some distance

TEMPEST Sources (ctd)

Printer and serial cables

Leakage into power lines

Coupling into power lines, phone lines, metal pipes

- Further radiation from there

Surface waves on coax lines

TEMPEST Protection

Extremely difficult to protect against

Stopping it entirely

- Extreme amounts of shielding on all equipment
- Run the equipment inside a Faraday cage

Stopping it partially

- FCC Class B computers and equipment
- RF filters on power lines, phone lines
- Shielded cables
- Ferrite toroids around cables to attenuate surface waves
- Radio hams have information on safely operating computers near sensitive comms gear

Use a portable radio as a simple radiation tester

Snake Oil Cryptography

Named after magic cure-all elixirs sold by travelling medicine salesmen

Many crypto products are sold using similar techniques

- The crypto has similar effectiveness
- This is so common that there's a special term, "snake oil crypto", to describe it

Snake Oil Warning Signs

Security through obscurity

- "Trust me, I know what I'm doing"
  - They usually don't
- Most security through obscurity schemes are eventually broken
  - Once someone finds out what your secret security system is, it's no longer a secret and no longer secure
  - It's very hard to keep a secret on the net

Proprietary algorithms and revolutionary breakthroughs

- "I know more about algorithm design than the entire world's cryptographers"
- Common snake oil warning signs are use of cellular automata, neural nets, genetic algorithms, and chaos theory
- See "security through obscurity"

Snake Oil Warning Signs (ctd)

Unbreakability

- Usually claimed by equating the product to a one-time-pad
- Product isn't a one-time-pad, and therefore not unbreakable

"Military-grade crypto"

- Completely meaningless term (c.f. "military-grade spreadsheet")
  - Military tends to use hardware, civilians use software
  - Prefer shift-register based stream ciphers, everyone else uses block ciphers
  - Keys are generally symmetric and centrally managed, everyone else uses distributed PKC keys
- Products should therefore be advertised as "nothing like military-grade crypto"

Snake Oil Warning Signs (ctd)

Technobabble

- Use of terms unknown to anyone else in the industry

Used by *xyz*

- Every product, no matter how bad, will gain at least one big-name reference customer

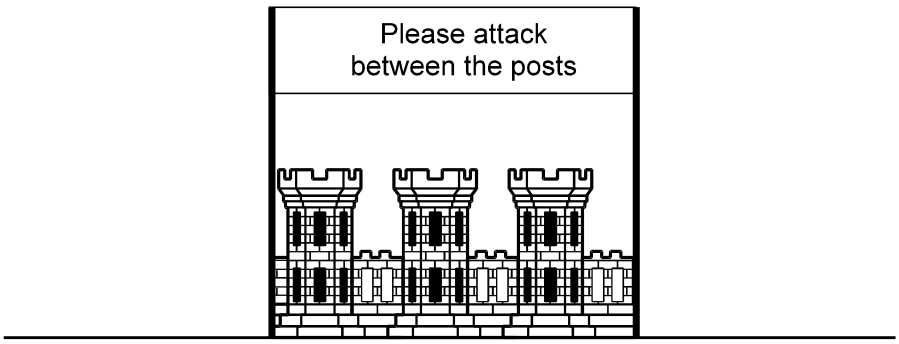
Exportable from the US

- Except for special-purpose cases (e.g. SGC), the US government in the past would not allow the export of anything that provided real security
- If it was freely exportable, it was broken

Snake Oil Warning Signs (ctd)

Security challenges

- Generally set up to make it impossible to succeed



- These things always get the media's attention, especially if the reward is huge (chance of press coverage = 20% per zero after the first digit)

Snake Oil Warning Signs (ctd)

Would you buy this product?

- "Our unbreakable military-grade bi-gaussian cryptography, using a proprietary one-time-pad algorithm, has recently been adopted by a Fortune 500 customer and is available for use inside and outside the US"

Badly marketed good crypto is indistinguishable from snake oil

- If you're selling a crypto product, be careful how your marketing people handle it
  - If left to their own devices, they'll probably sell it as snake oil

Snake Oil in the Media

Magazine reviews are a poor gauge of software security

WinXFiles (trivially broken file encryption)

- PC Answers: Listed in "10 proven security programs"
- Windows News: Listed in "75 best Windows utilities"
- FileMine: Rated as a Featured Jewel
- Shareware Junkies: 5 stars, "a must have for anyone sharing a computer with files they want to keep private"
- PC Format: "Unbeatable and excellent file encryption"
- TUCOWS: Rated 4 cows
- Ziff-Davis Interactive: 5 stars, "keeps files and data on your PC as safe as if they were under lock and key"

more

Snake Oil in the Media (ctd)

continued

- The Windows95 Application List: “an excellent application for protecting your personal files”
- RocketDownload: Four smilies
- “Simply the Best” site award

One major publication once rated a collection of encryption programs by how good the user interface looked

Snake Oil Case Study

Meganet Virtual Matrix Encryption

- “A new kind of encryption and a new algorithm, different from any existing method”
- “By copying the data to a random built-in Virtual Matrix, a system of pointers is being created. ...”
- “The worlds first and only unbreakable crypto”
- “We challenged the top 250 companies in the US to break our products. None succeeded”
  - They don’t even know that Meganet exists
- “55,000 people tried to break our product”
  - 55,000 visited their web page
- “Working on standardising VME with the different standards committees”

Snake Oil Case Study (ctd)

Challenged large companies to break their unbreakable crypto

- Enumerate each company in the PR to ensure that their name is associated with large, publicly held stocks

Used accounts at organisations like BusinessWire and PRNewswire to inject bogus press releases into newswires

- Run anything at $500 for 400 words
- Claimed IBM was so impressed with their product that they were recommending it for the AES
  - IBM had never heard of them

Snake Oil (ctd)

Big-name companies sell snake oil too

Tools exist to recover passwords for

- Adobe Acrobat/PDF
- ACE archives
- ACIUS 4th Dimension
- Arj archives
- Clarion
- Claris Filemaker Pro
- CompuServe WinCim
- dBASE
- Diet compressed files
- Eudora
- ICQ
- Lotus 1-2-3

Continues

Snake Oil (ctd)

Continued

- Lotus Ami-Pro
- Lotus Organiser
- Lotus Symphony
- Lotus WordPro
- LZEXE compressed files
- MS Access
- MS Backup
- MS Excel
- MS Mail
- MS Money
- MS Outlook
- MS Project
- MS Scheduler

Continues

Snake Oil (ctd)

Continued

- MS Word
- MYOB
- Norton Secret Stuff
- Paradox
- Pegasus Mail
- Pklite compressed files
- Pkzip archives
- Q&A Database
- Quattro Pro
- QuickBooks
- Quicken
- Stacker
- Symantec Act

Continues

Snake Oil (ctd)

Continued

- Trumpet Winsock
- VBA projects
- WinCrypt
- Windows 3.1/95/98 passwords
- Windows Dial-up Networking (DUN)
- Windows NT/2000 passwords
- WinXFiles
- WordPerfect
- WS FTP

... and many, many more

Selling Security

Security doesn't sell well to management

Many security systems are designed to show due diligence or to shift blame

- Crypto/security evidence from these systems is very easy to challenge in court

You get no credit if it works, and all the blame if it doesn't

To ensure good security, insurance firms should tie premiums to security measures

- Unfortunately, there's no way to financially measure the effectiveness of a security system

Selling Security to Management

Regulatory issues

- Liability for negligence (poor security/weak crypto)
- Shareholders could sue the company if its share price drops due to a security breach
- US companies spend more on security than non-US ones due to litigation threats

Privacy/data protection requirements

Media stories of hacker/criminal attacks on systems

The best security customers

- Have just been publicly embarrassed
- Are facing an audit

TCSEC/Orange Book

Trusted Computer Security Evaluation Criteria

- Based on 10-15 years of security research
- Usage model: multiuser mainframes, terminals/users cleared at a single level
- "Make it simple enough that even a general can understand it"
- Attempts to apply it to other areas (e.g. networks) via increasingly tortuous "interpretations"

Applying the Orange Book

Maximum sensitivity	Rmax
Unclassified (U)	0
Unclassified but sensitive (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS)	5

Minimum user clearance	Rmin
Uncleared (U)	0
Uncleared, allowed access to sensitive information (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS)/Background Investigation	4
Top Secret (TS)/Special Background Investigation	5

Risk Index = Rmin – Rmax

Applying the Orange Book (ctd)

Risk index	Operating Mode	Orange Book class
0	Dedicated	None
0	System high	C2
1	Limited access, controlled, compartmented, multilevel	B1
2	Limited access, controlled, compartmented, multilevel	B2
3	Controlled, multilevel	B3
4	Multilevel	A1
5	Multilevel	?

Applying the Orange Book (ctd)

Operating modes

Dedicated	System exclusively used for one classification
System high	Entire system operated at and all users cleared at highest sensitivity level of information
Limited access	All users not fully cleared or authorised access to all data
Controlled	Limited multilevel
Compartmented	At least one compartment requiring special access to which not all users have been cleared, but all users cleared to highest level
Multilevel	Two or more classification levels, not all users cleared for all levels