TDC 375 – Network Protocols
TDC 563 – P&T for Data Networks

Miscellanea
Scanning strategy

- You could use something like nmap/zmap
- custom code and solutions
  - two-stage SYN scan with follow up app check
  - post-process pcap or real-time data extraction
- Embedded scan signatures and fingerprints
- How do you probe the entire Internet?
- Do you white list prefixes?
- Responding to and limiting complaints
X.509 certificate properties

• Time stamps
• Discovery time, valid/expiry times
• Address, port
• Certificate in PEM format
• Serial, version, hash signature
• Issuer detail
• User detail (subject, organization, email etc)
X.509 insight ideas

- Subject and Alt host names
- Email addresses
- Expiry times
- Algorithms used
- Duplicate certificates
- Patterns of certificates used by common software
Public key infrastructures (PKIs)

• X.509 certificates
• DNSSEC
• PGP
• Successes and challenges
  • Commercial costs and viability
  • Ease of use, complexity and user perception
IPsec, VPNs and tunnels

• Confidentiality, integrity and replay protection
• Deployment challenges, e.g. NAT
• E2E versus Net2N or Net2E
• Hardened boundaries and soft gooey fillings
Tor

- An anonymity-enhancing relay network
- Clients connect to an entry or bridge
- Retrieve a relay node directory
- Build a path, only client knows the full path
- Leverages proxy, X.509 and SSL/TLS technology
- Challenges and issues
- Related technologies
The end-to-end Argument

- Where do you place functionality?
  - The paper doesn't "specify" it provides a framework on how to arrive at a decision
- It does NOT insist on a "stupid" network
- Key phrase: “A great deal of information about system implementation is needed to make this choice intelligently.”
- Many modern technologies, and often entire nets, are often incompatible with an e2e design.
- How to reconcile e2e with the modern Internet?
Rent to pwn

A "rented" skimming set is merely the same set but you do not get the Encryption key.

You send us the tracks immediately after getting them, we decode, cash out approx half

The cost of the rental units are €900

After 1 use, it is yours, as we will have made more than enough money to cover our costs.
$$\text{MAKE MONEY FAST}$$

<i>but i've been talking to people high up in banking and they've basically told me no wire above $50,000 will probably go through so i'd be looking at wiring below that amount</i>

<i>i have access to accounts ranging from a few hundred thousand to several million that i have the ability to wire from</i>
IPv6 skiddies

A> I DDOS PPL ALL THE TIME IN HERE
A> im gonna have to refrain you from openly ddos ppl in this chan
A> ipv6
A> so none u fucks can get me

B> had ipv6
B> i got a few roots with ipv6
B> udp6.pl
B> will pwn you
B> you cannot refrain me from anything
A> Yo is this your company
A> that sells these fake watches?
...
A> Hook me up w/ a cc once in awhile
...
A> 3/4k a day?
A> Get me in on this
A> I'd quit bots 2 make 4k$ a day
Spam in the market place

RULES: @/+v verify first, | For cashout join #Cashout | Report/View rippers #rippers –/– For Help join #help –/– For WesternUnion Join #WesternUnion Notice: Only English

A> selling php maler send to inbox yahoo/gmail, paypal unverified balance 100$, blocked egols, cc, payment egold

A> selling php mailer send to inbox yahoo/gmail, hackhost+cpanel, inbox, fresh cc, paypal unverify, r57+c99 shell, payment egold
The ugly and unmentionables

The Internet Underground is like the traditional criminal underground. All sorts of things can be bought (weapons), sold (drugs), traded (credit cards), obtained (passports) and found ([REMOVED]) there.
On that positive note!

Enjoy your holiday and new year break!
You know where to find me.

jtk@depaul.edu