Registry Vulnerabilities
An Overview

Edward Lewis
ed.lewis@neustar.biz
ccNSO Tech Day @ ICANN 46
April 8, 2013
Goal of the Presentation

» High-level overview of where security matters
  » Reduce the chances that something (big) is missed
  » To help identify how other presentations can help
What is Security?

» Component of reliability, availability
  » Available means being “up”
  » Security means “not being taken down” or “corrupted”

» Security blends with general availability issues
  » What’s covered here is related to malicious threats, not environmental threats (like power outages)
What Does Security Do?

» Limits the damage caused by malicious(-like) activity

» Never prevents an attack
  » To attack or not is someone else’s decision

» Not absolute
  » What an attacker is willing to do versus how well a defense is constructed

» “Risk management”
Where To Start?

» What needs protecting?
» How much can be allocated to defense?

» Analyze the operation (architecturally)
» Define the normal states of operation
» Define what activity represents a risk and monitor
» Automate responses and clean up
Where To Stop?

» Needed but not desired
  » Balance!

» Avoid
  » Preventing valid uses of the network
  » Becoming a burden on legitimate users

» State goals in planning so “done” can be accomplished
  » Done being “good enough for now”
What Is Most Important

» A registry’s role is to match objects to entities
  » Reliably, always available

» Domain Name Industry
  » Mapping domain names to registrants
  » In DNS time
  » Enforcement of policies

» For Number Resources (the RIRs)
  » Except that the names are numbers (IP, AS)
  » The rest is the same
Think About Normal

» The heart is “the” database

» Services provided surrounding this database
  » To input data (provisioning)
  » To export data (e.g., DNS)
  » How do these interact on a “as expected” basis?

» Specifics can differ from registry to registry
Domain Name Registry

An Ecosystem View
Provisioning Services

- Customers
- Registration
- Web
- Billing
- Database
- “Rules”
- Regulator
Reporting Services

Database

Whols

DNS

DNSSEC

The Internet
Basic Security

» All organizations must have basic security
  » Physical security such as locks, video cameras
  » Financial security such as business continuity
  » Personnel security such as “HR” rules and regulations
  » Information Technology security such as firewalls

» And make sure it works
  » Security audits
  » Penetration tests, other security exercises
When All Else Fails, Escrow

» If everything else comes “crashing down”
  » A well planned escrow system is needed

» Escrow means a copy of the database held in a secured location away from the registry

» Test escrow
  » But hope to never use it!
Provisioning Services

» The Registration Interface
  » This might be EPP (doesn’t have to be)

» General Information Website
  » Low-profile but a service nonetheless

» Billing
  » Not often considered by engineers
Provisioning Vulnerabilities

» Denial of Service or “Hogging”
  » Access has to be guaranteed for customers
  » Need to prevent one from blocking out others

» Poorly formatted Data
  » Such as an “SQL injection” attack

» “Corrupt” Data
  » Stolen credentials
  » Fraudulent registrations
Techniques

» For registry website
  » Basic security

» For registration protocol
  » Traffic shaping
  » Restricting addresses

» For poorly formatted data
  » Better software, proven tools, limit testing

» For corrupt data
  » Business transaction security
  » Malicious domain name takedown process
For Billing

» Protect credit card numbers (if applicable)!
  » Learn about the PCI Security Standards Council

» Protect any kind of account information
  » An attack might target the accounts of customers
  » Or the attack might use stolen credits to register names
Internal Systems

» Database
  » Contains the resource to holder mapping
  » Might contain contact information
  » Might contain credentials
  » Contains all other needed operational information

» Business rules enforcement
  » Who is allowed to register what
  » What enforcement is needed?
Database Threats

» Beyond fraudulent data

» Structure database appropriately

» Limit access by anyone, even staff
  » Even “read only”
  » Limit “insider attacks”
  » Limit damage from “social engineering” – persuading staff to give out information that should not be reported
“Rules”

- Ensure they are properly followed
- Available and functioning
- Work with regulators to ensure policies are sensible, well understood and achieving the right goals
Reporting Services

» Whols
  » Directory Inspection/Access Services

» DNS
  » The reason for all of this work

» DNSSEC
  » Key management is new
  » HSM or not?
WhoIs Threats

» TCP based attacks
   » Well understood, not so scary anymore

» Data Mining

» For some registries, WhoIs is not a target
   » Bulk access is provided within terms of use
   » “Abusing” WhoIs is just “annoying”
Whols Defenses

» Host security for TCP issues
» General availability techniques (multiple sites, servers)
  » Rate limits when a source is a nuisance

» For data mining
  » Bulk access agreement limiting data use
  » Captcha in the UI
  » Monitoring and throttling of requests
DNS Threats

» Popular target
  » Denying service by knocking out servers
    » “Kill packets” are possible
  » Packet flood attacks (DDoS)
    » Registry as victim
    » Registry as unwitting accomplice
  » Cache Poisoning
    » Not a threat to registry servers, but registries can help limit it

» Data Disclosure
  » Some jurisdictions consider the list of domains sensitive
Reflection/Amplification Attack

» One class of attacks uses registries as unwitting accomplices.

Attacker
Small DNS query
False return address

DNS
DNSSEC

Victim
Large DNS response
What Does This Mean to DDoS

» Traditionally plans assume that one is the victim
  » Can my systems withstand a DDoS attack?
  » Do I need more capacity?

» Reflection attacks change this
  » More capacity might mean more ammunition for the attack

» What an operator can do now
  » Rate Limiting, specifically Response Rate Limiting, now implemented in various distributions: BIND, NSD, Knot
DNS Defenses

» Host security, up to date/customized name server code

» Dispersed set … limit shared fate

» Anycast can isolate attack regions

» Rate limiting of responses

» DNSSEC
DNSSEC Considerations

» The key management function
  » Many documents dedicated to this topic (e.g. US NIST)

» DNSSEC private key material has to be kept a secret
  » Poorly derived
  » Exported via an employee, lost hardware
  » Crypt-analysis

» Signature generation process
  » False data submitted for signing
DNSSEC Techniques

» Use of NSEC3 or NSEC

» Choose parameters well, decide on workload
  » Too much, it’s a burden
  » Too little, it’s forgotten

» HSM or not?
  » Data is more important than the private key
  » Complicate “high availability” plans
DNSSEC and Amplification

» Improvements make it more useful to malicious use
  » IPv6, more data
  » DNSSEC
  » Larger NXDOMAIN responses

» What can be done?
  » Ignore DNSSEC and go insecure is not a desirable choice
  » Look for ways to limit size of responses
    » Be efficient on records, choose key sizes wisely
  » Response rate limiting
Conclusion

» There are a lot of “attack surfaces” in a registry
» There are a lot of techniques in defense

» Security needs to be planned ahead of time
  » Too little and - panic
  » Too much and - inhibiting

» …Questions?