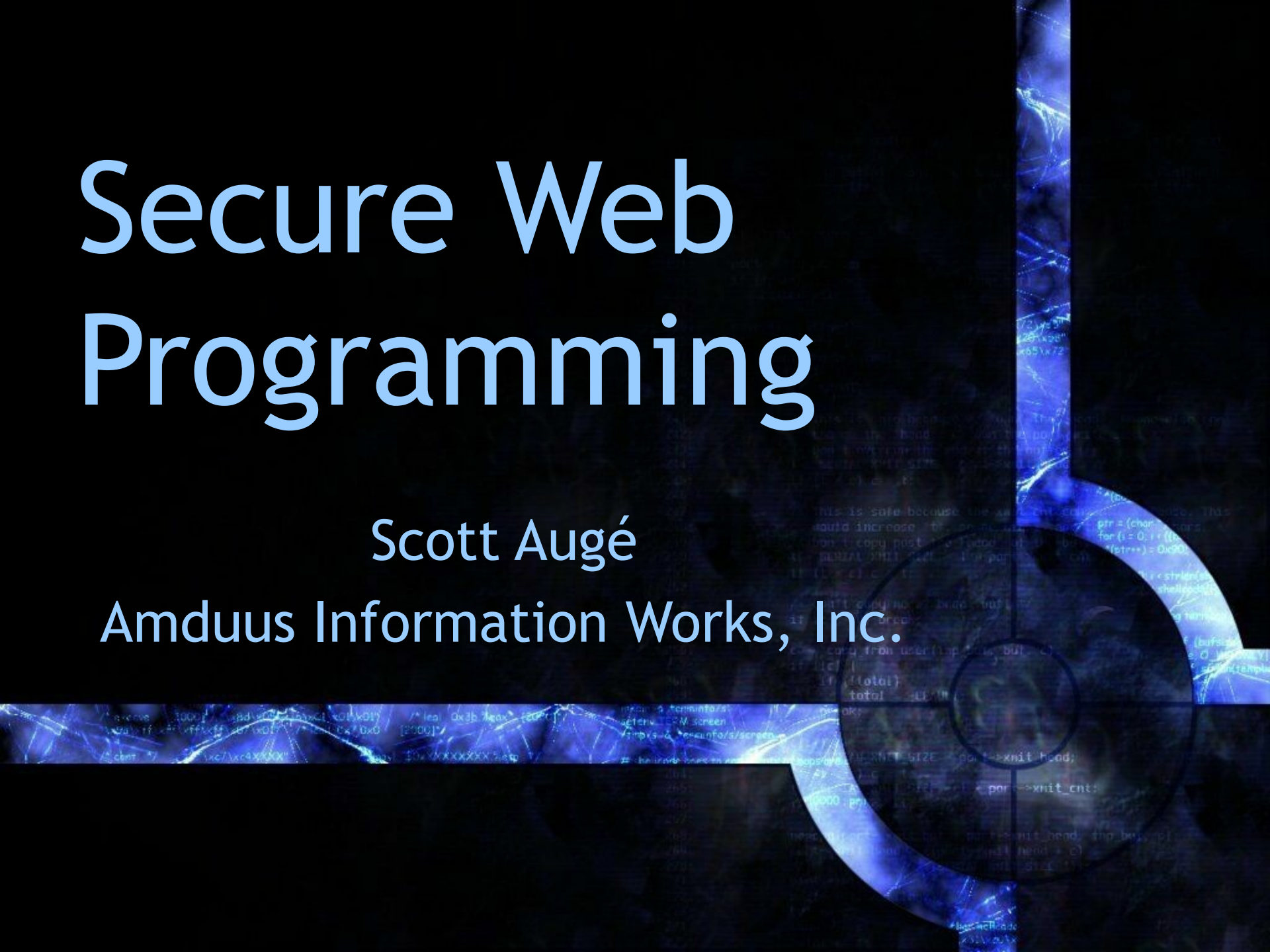
Secure Web Programming

Scott Augé

Amduus Information Works, Inc.

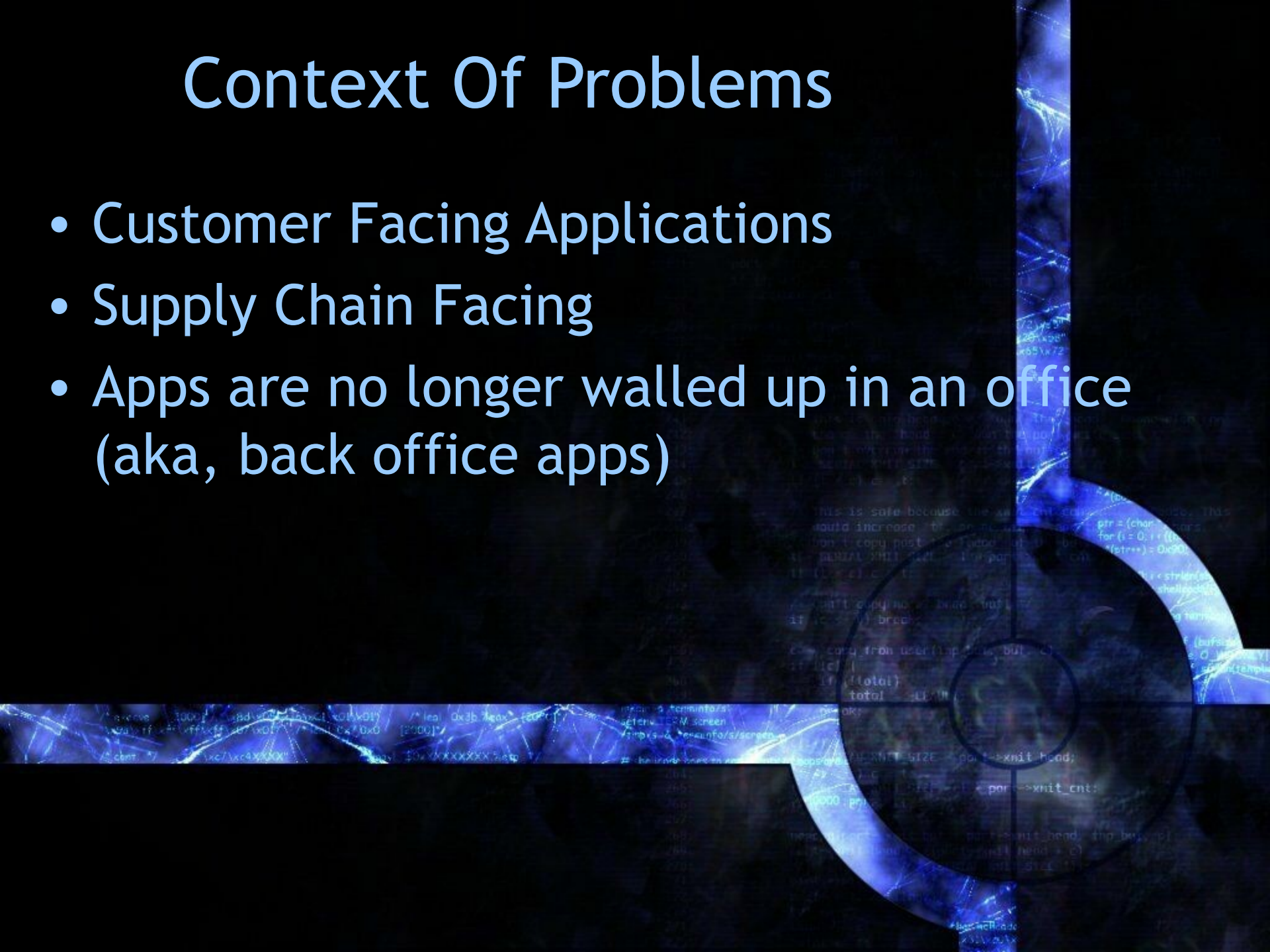


Welcome

- Amduus has been in business for 10+ years.
- Multiple languages
- Multiple Operating Systems
- Customer Facing Apps
- SAAS/Self-Hosted

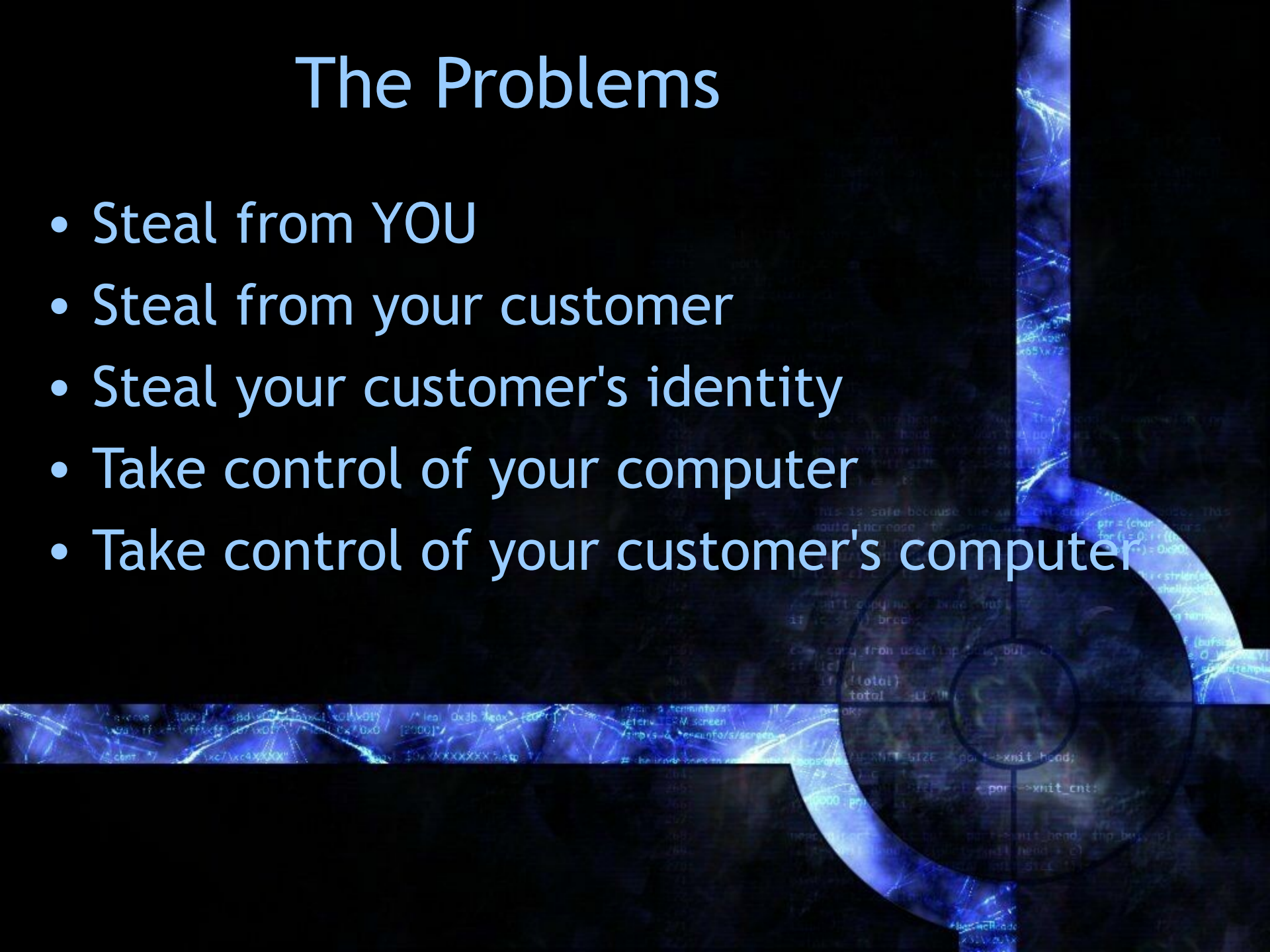
Context Of Problems

- Customer Facing Applications
- Supply Chain Facing
- Apps are no longer walled up in an office (aka, back office apps)



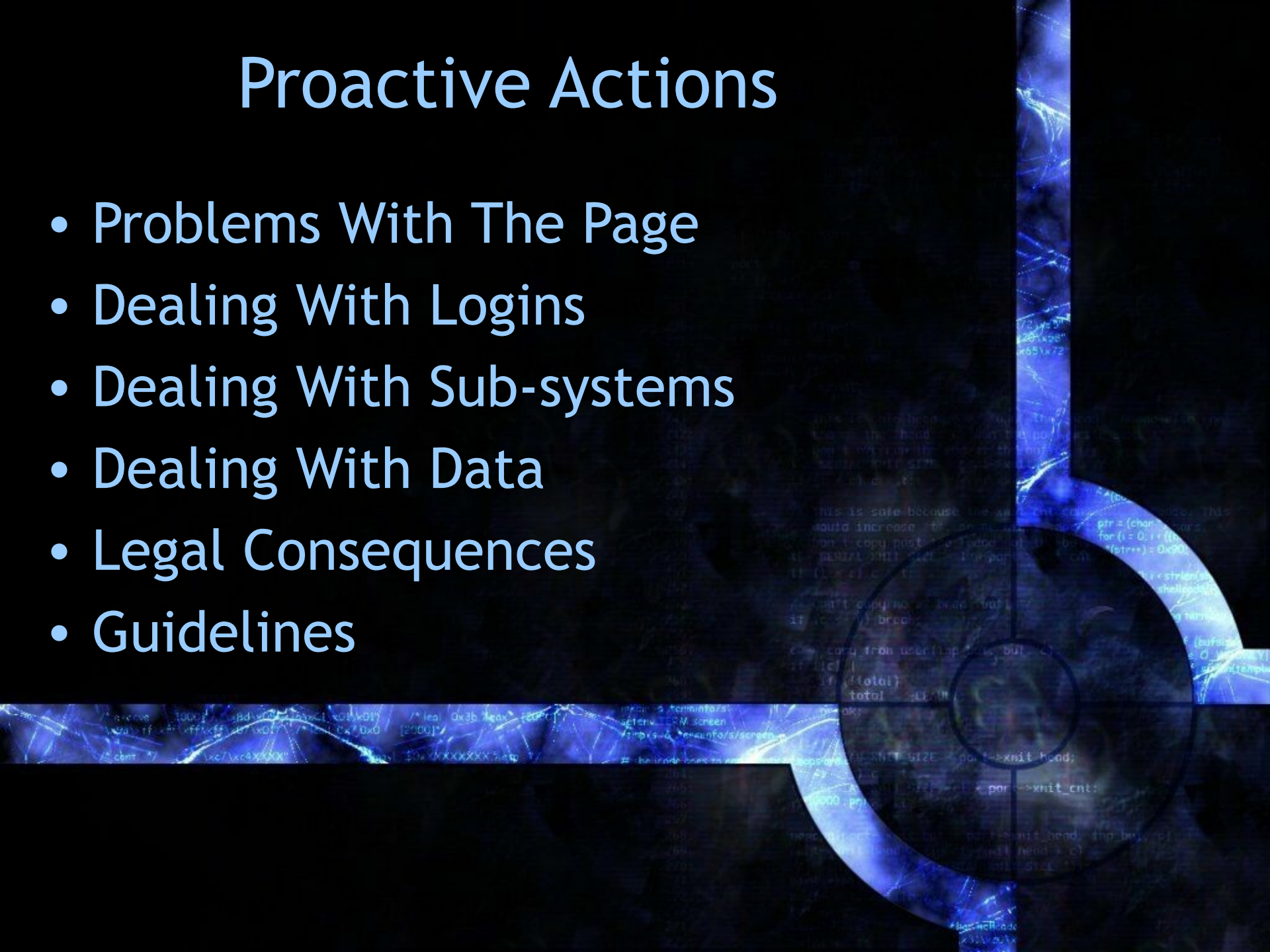
The Problems

- Steal from YOU
- Steal from your customer
- Steal your customer's identity
- Take control of your computer
- Take control of your customer's computer



Proactive Actions

- Problems With The Page
- Dealing With Logins
- Dealing With Sub-systems
- Dealing With Data
- Legal Consequences
- Guidelines

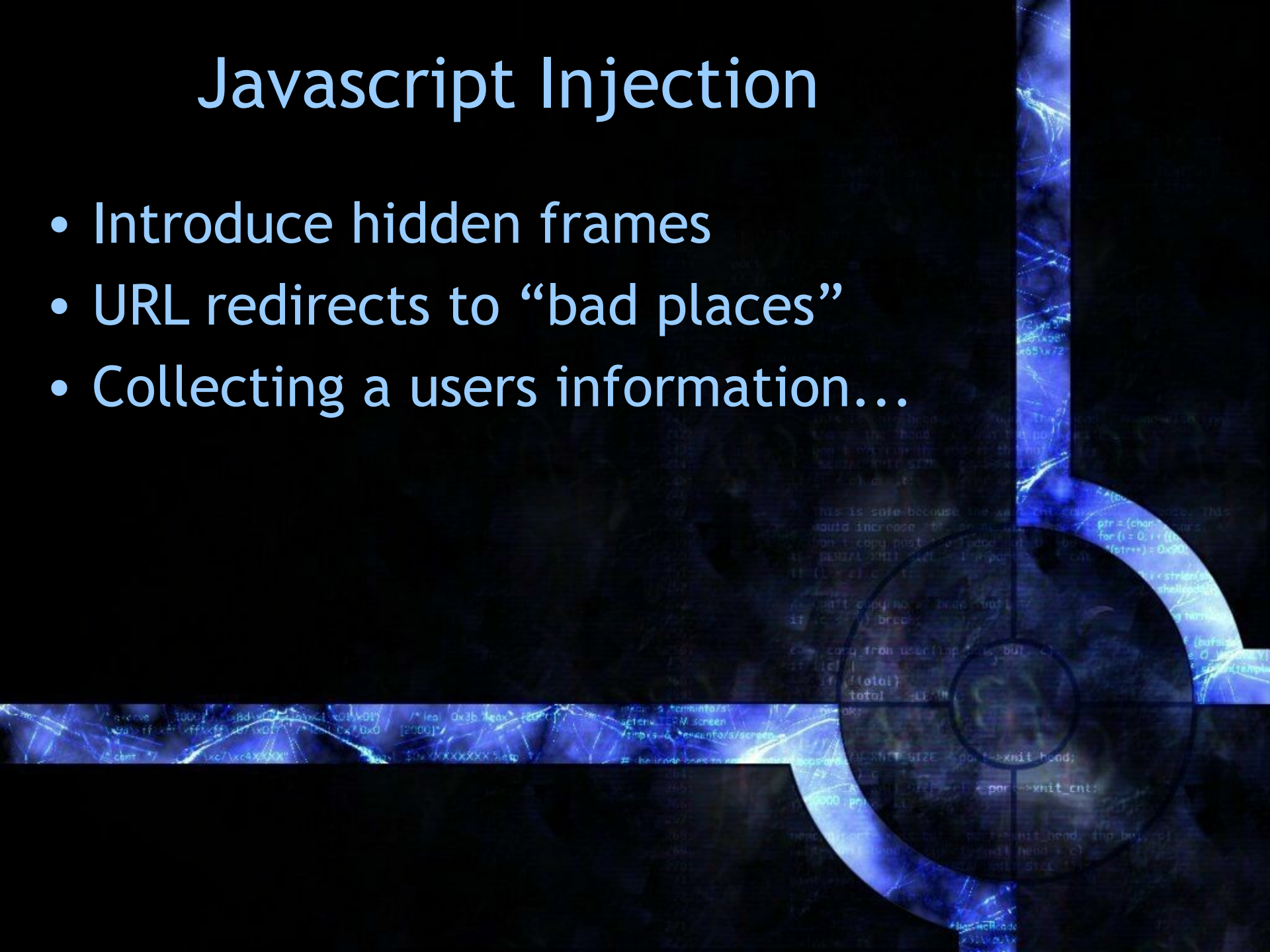


Javascript Injection

- User inputs javascript in an input field
- When displayed, javascript ends up on readers page
- Not a Webspeed problem – sometimes it is desired behavior!
- PHP, C, C++, Other Languages have same problem

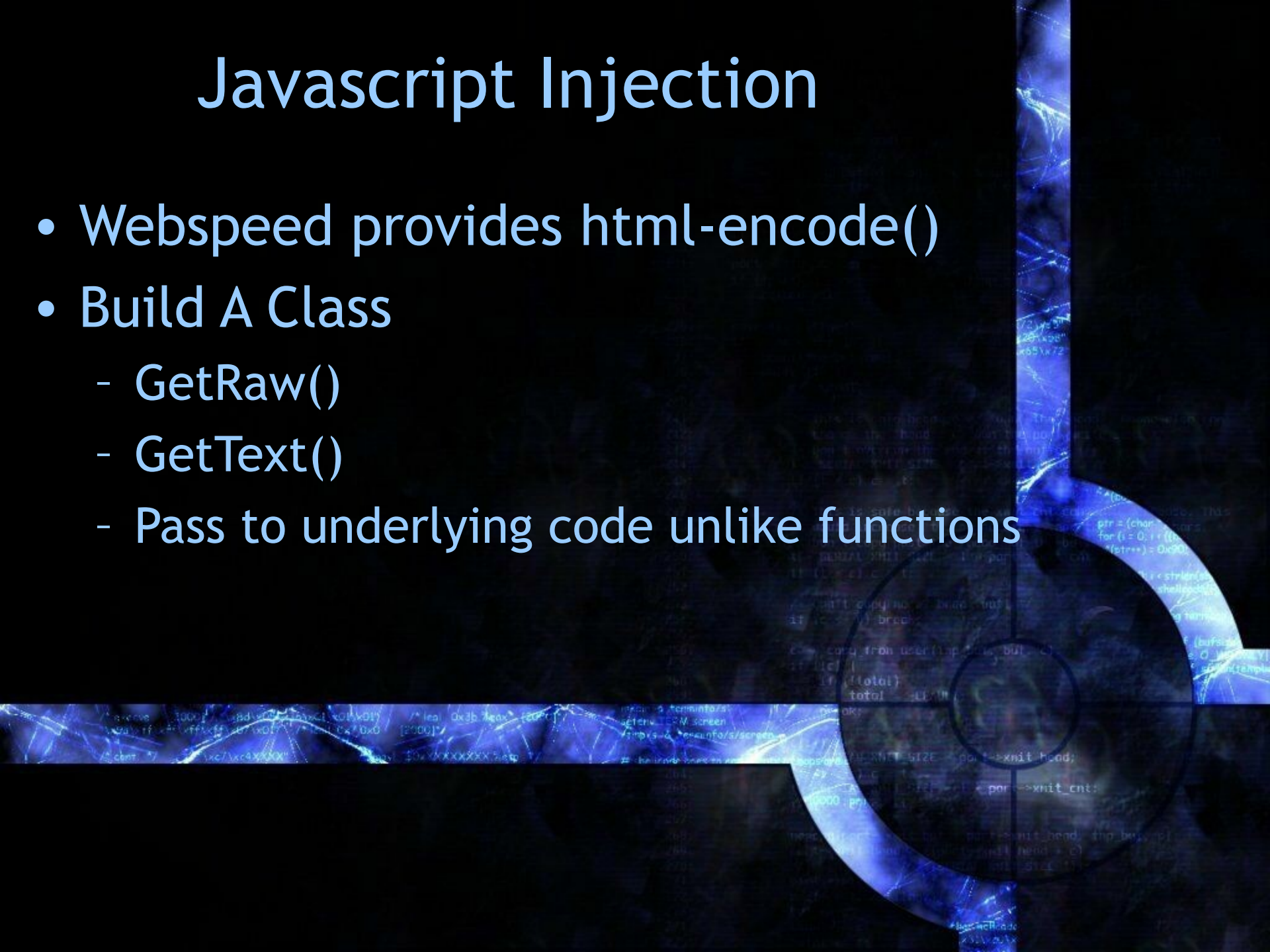
Javascript Injection

- Introduce hidden frames
- URL redirects to “bad places”
- Collecting a users information...



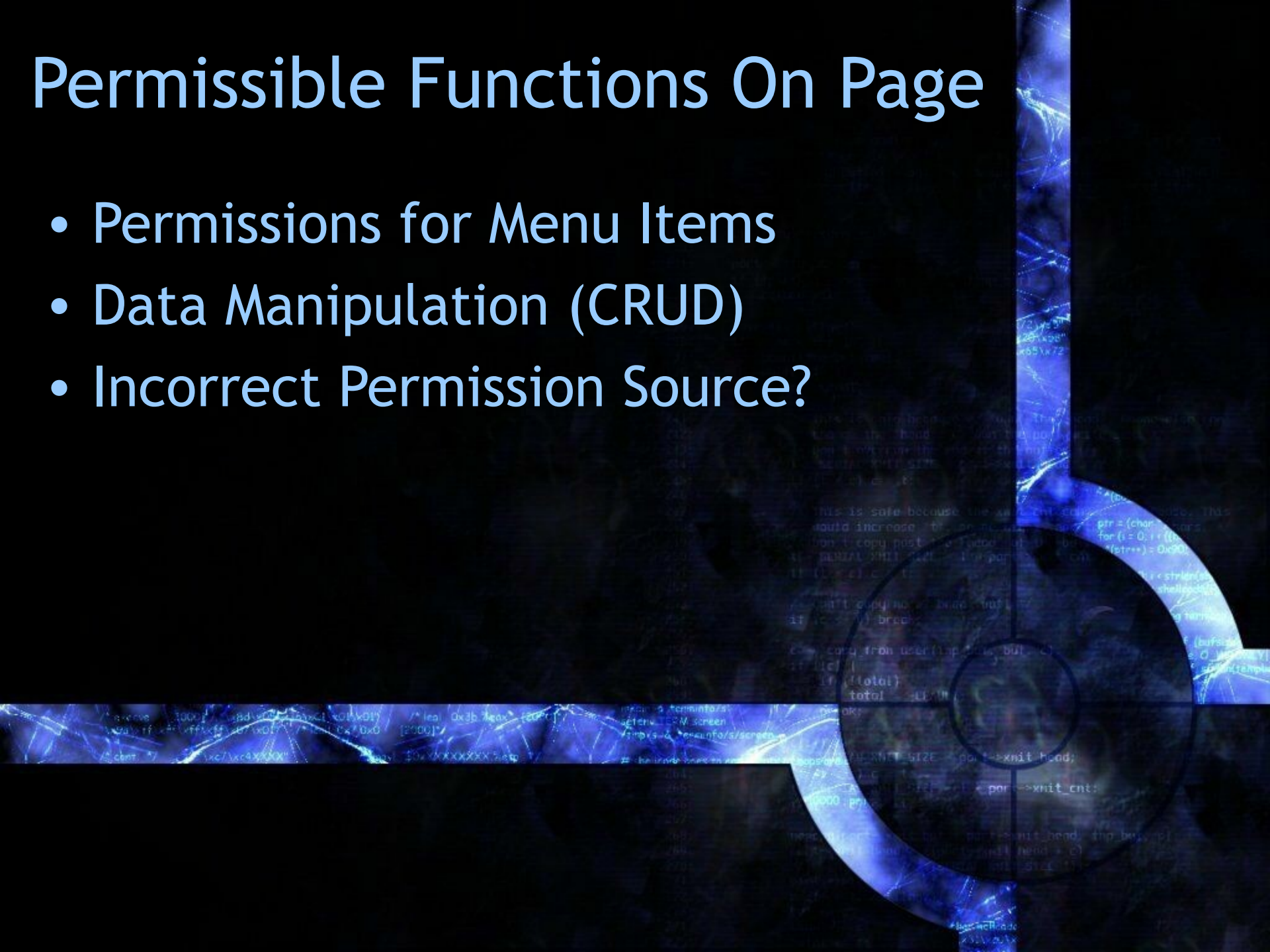
Javascript Injection

- Webspeed provides html-encode()
- Build A Class
  - GetRaw()
  - GetText()
  - Pass to underlying code unlike functions



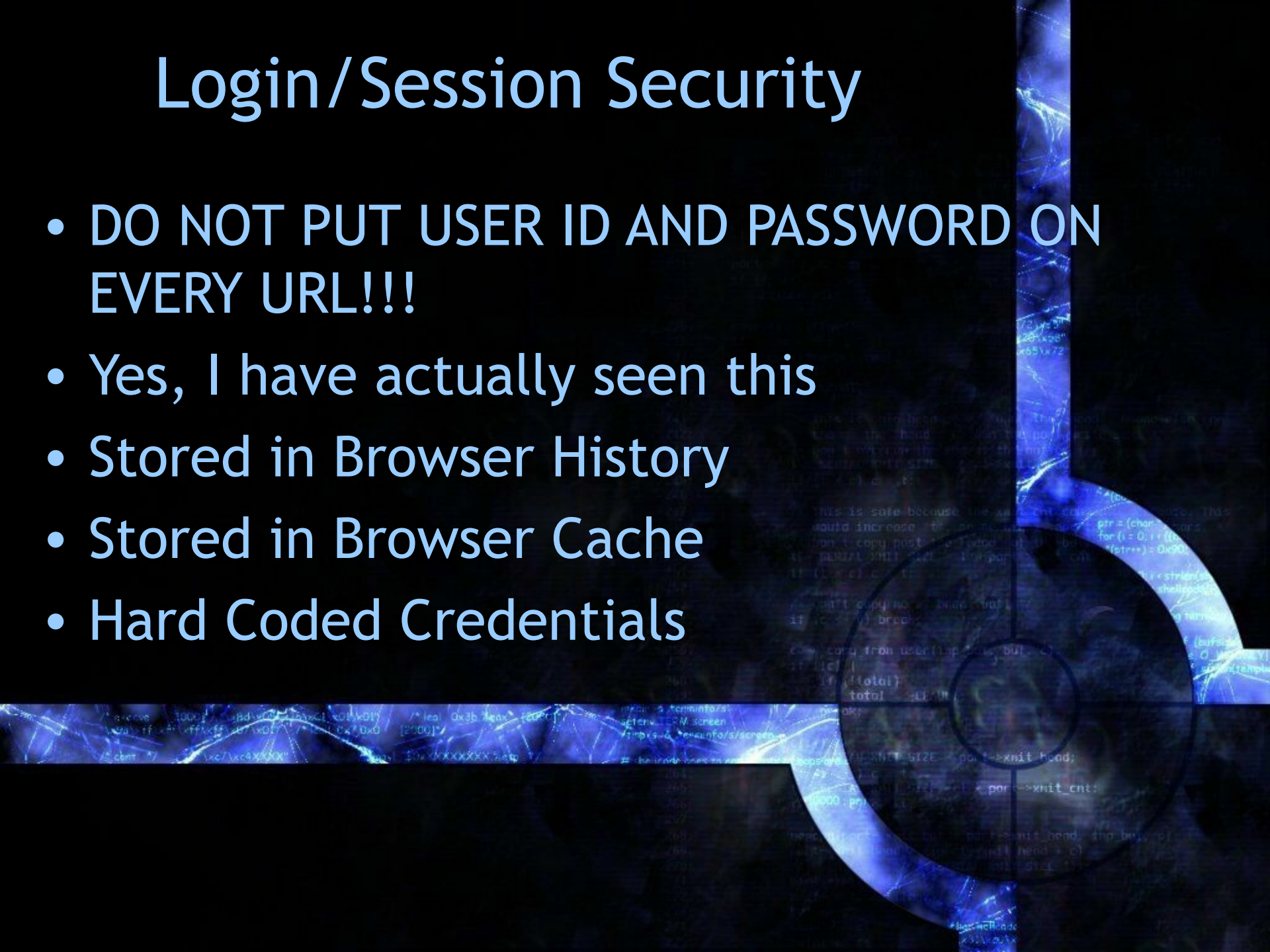
Permissible Functions On Page

- Permissions for Menu Items
- Data Manipulation (CRUD)
- Incorrect Permission Source?



Login/Session Security

- DO NOT PUT USER ID AND PASSWORD ON EVERY URL!!!
- Yes, I have actually seen this
- Stored in Browser History
- Stored in Browser Cache
- Hard Coded Credentials



Login/Session Security

- Use Random String Cookie for Session ID
  - Relate string to database record
  - Database record has actual user identity
  - Database record has LastUsed field
  - Allows Auto Logout
- Use a class for session info like IsLoggedIn(), Logout(), Login()...

Login/Session Security

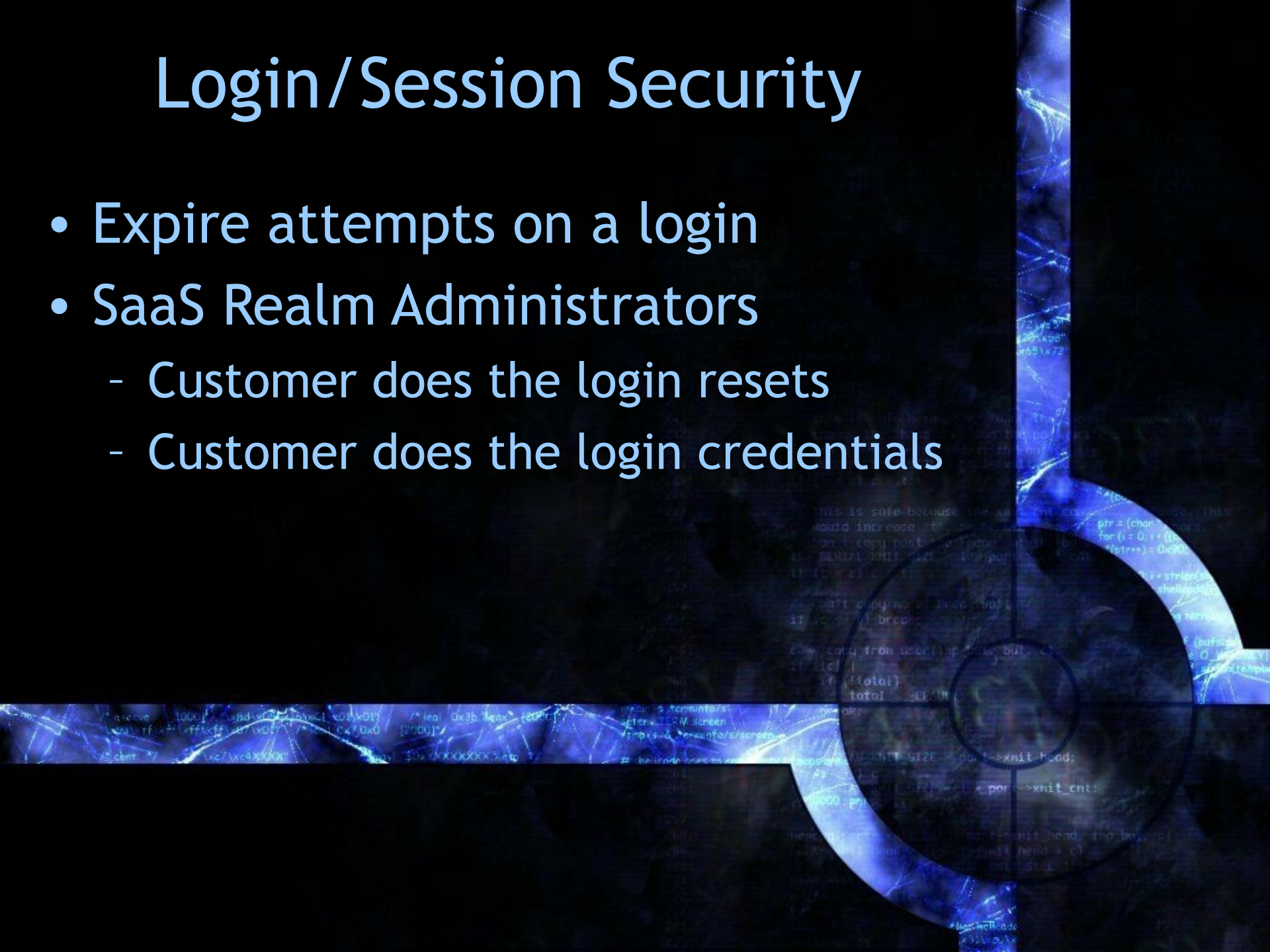
- Often useful to use a web service behind the application for this
- Web service allows different groups of apps, and upgrades
- Encrypt the passwords!
- Enforce password complication!

Login/Session Security

- Control Access by REMOTE_ADDRESS
  - Provides An Immediate Stopping Point
  - User/IP List for multiple devices
  - Control what addresses can do anything on the site
- Use source DNS in a similar manner

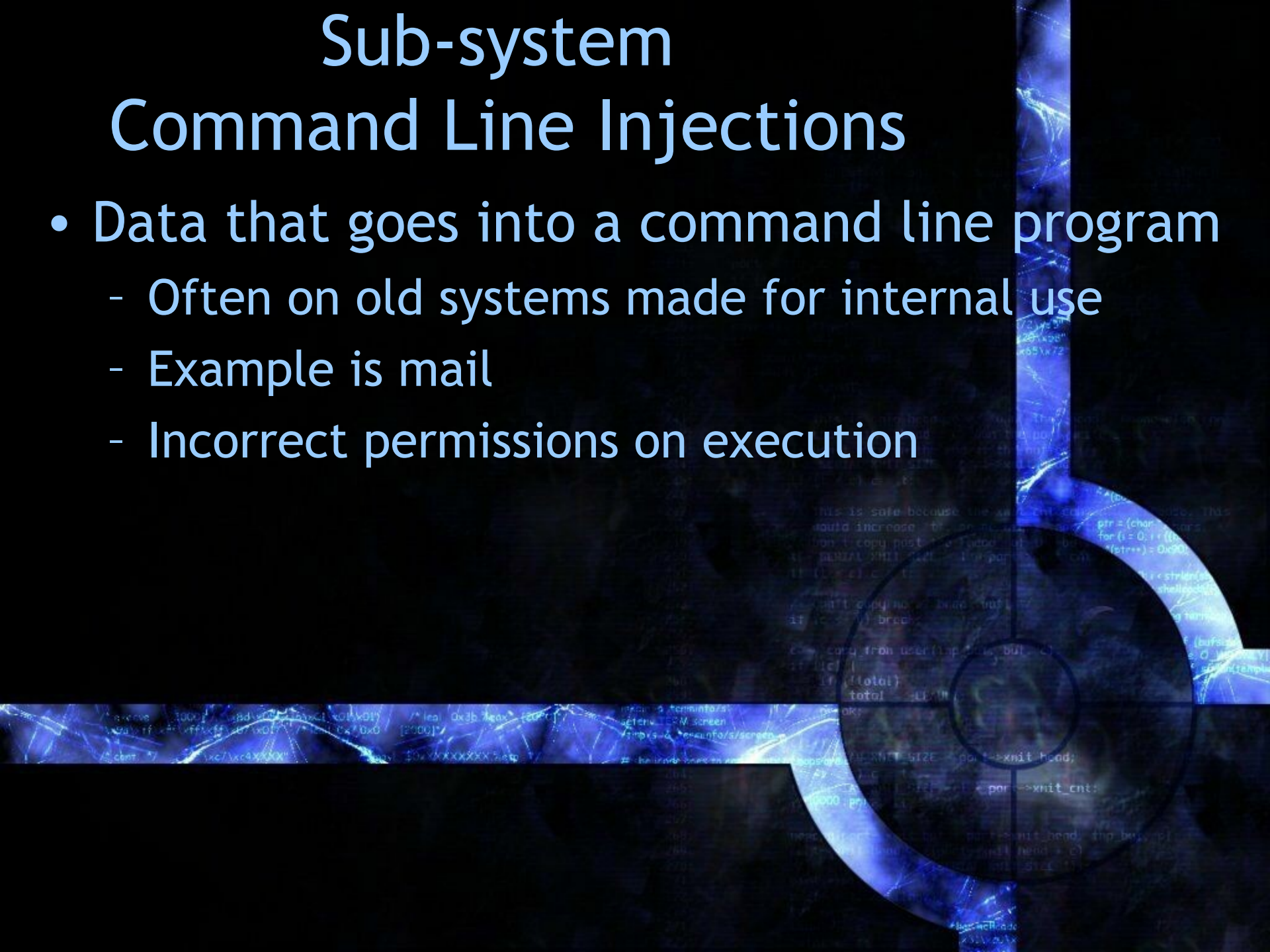
Login/Session Security

- Expire attempts on a login
- SaaS Realm Administrators
  - Customer does the login resets
  - Customer does the login credentials



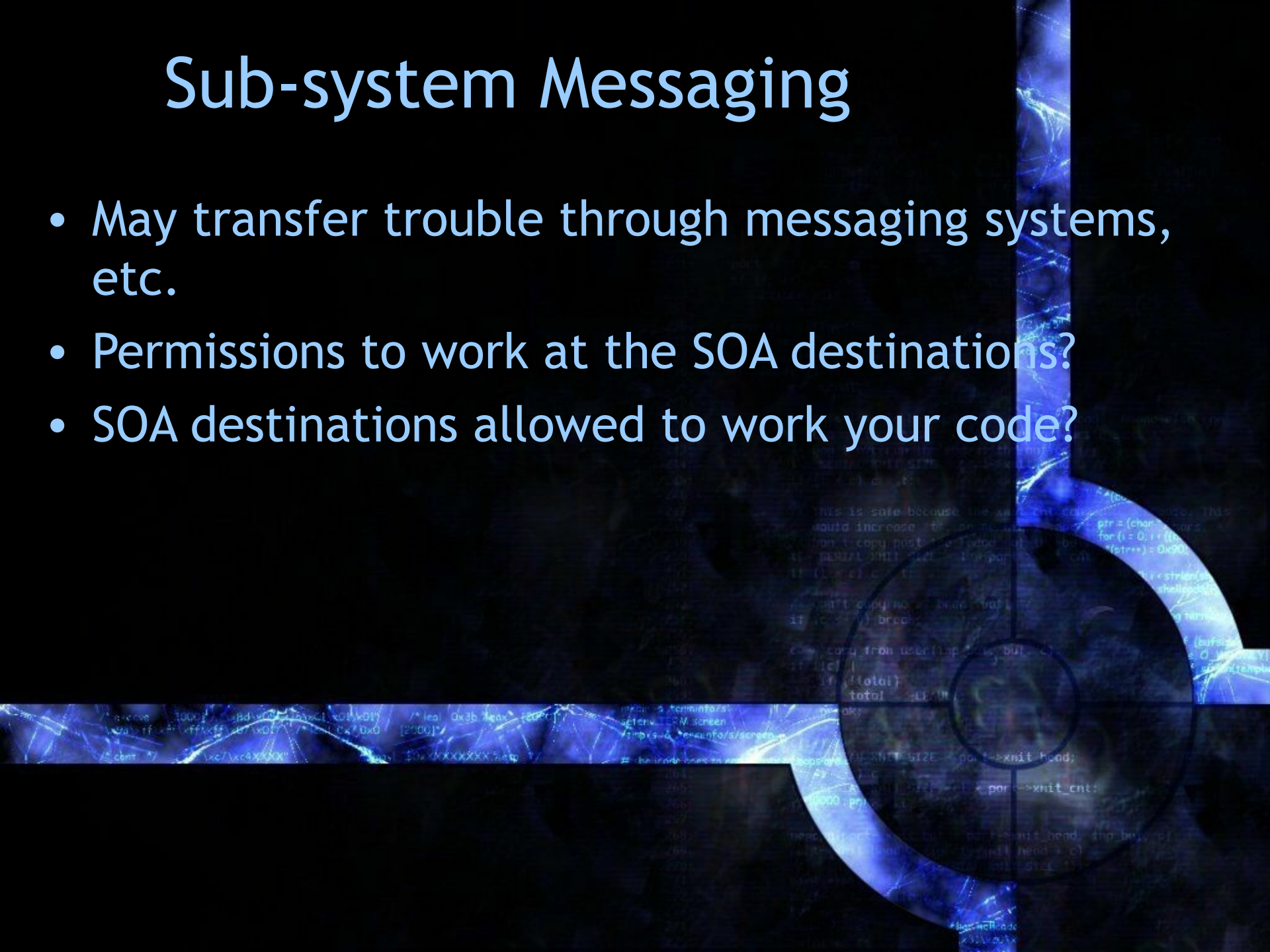
Sub-system Command Line Injections

- Data that goes into a command line program
  - Often on old systems made for internal use
  - Example is mail
  - Incorrect permissions on execution



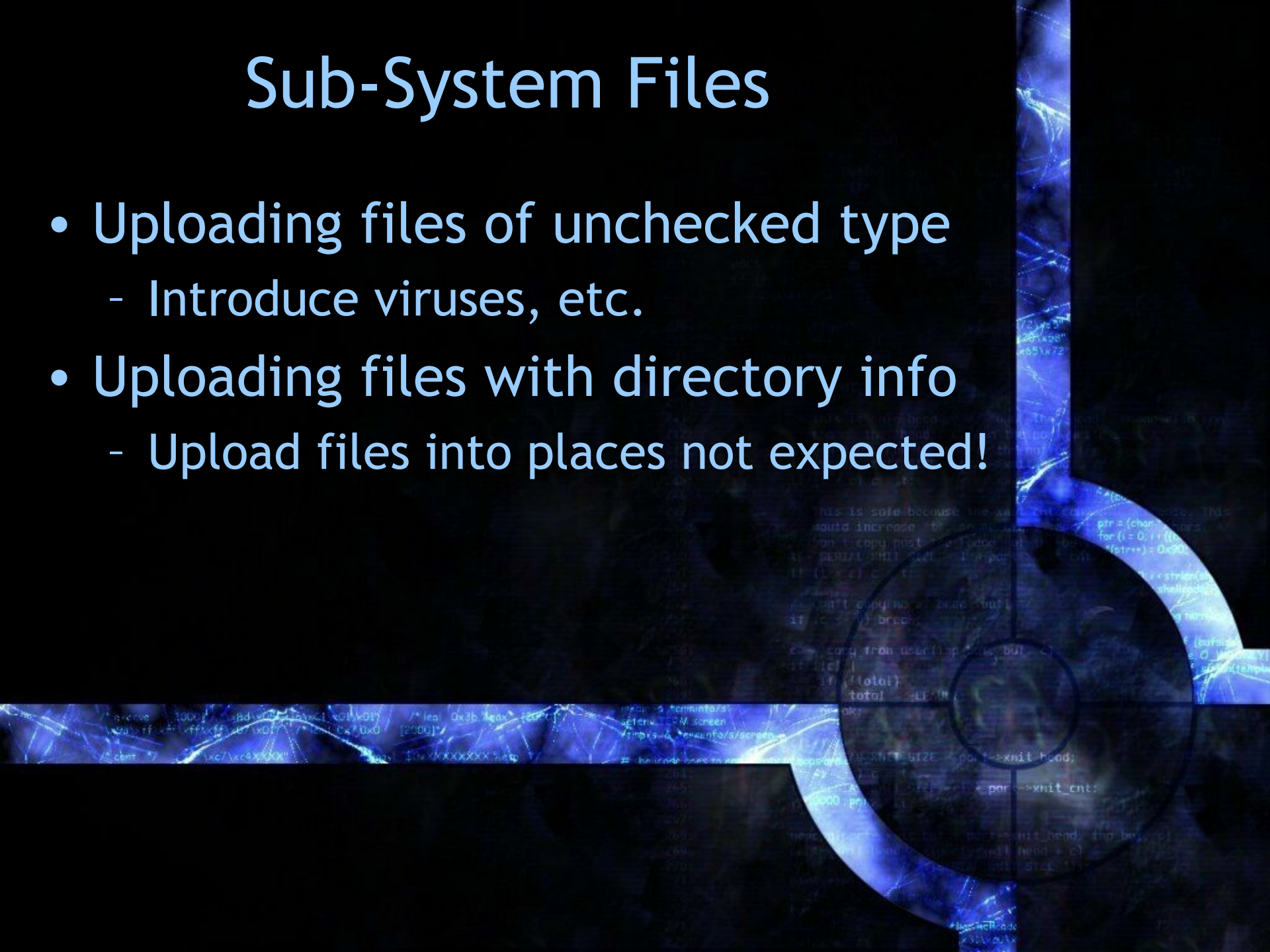
Sub-system Messaging

- May transfer trouble through messaging systems, etc.
- Permissions to work at the SOA destinations?
- SOA destinations allowed to work your code?



Sub-System Files

- Uploading files of unchecked type
  - Introduce viruses, etc.
- Uploading files with directory info
  - Upload files into places not expected!



Dealing With Data

- Do not use easily identifiable data for record identifiers
  - Nothing sequential
  - Nothing short
  - Perhaps hash of unchanging data fields + changing “salt”
  - Specific field with large random string and on an index + “salt”

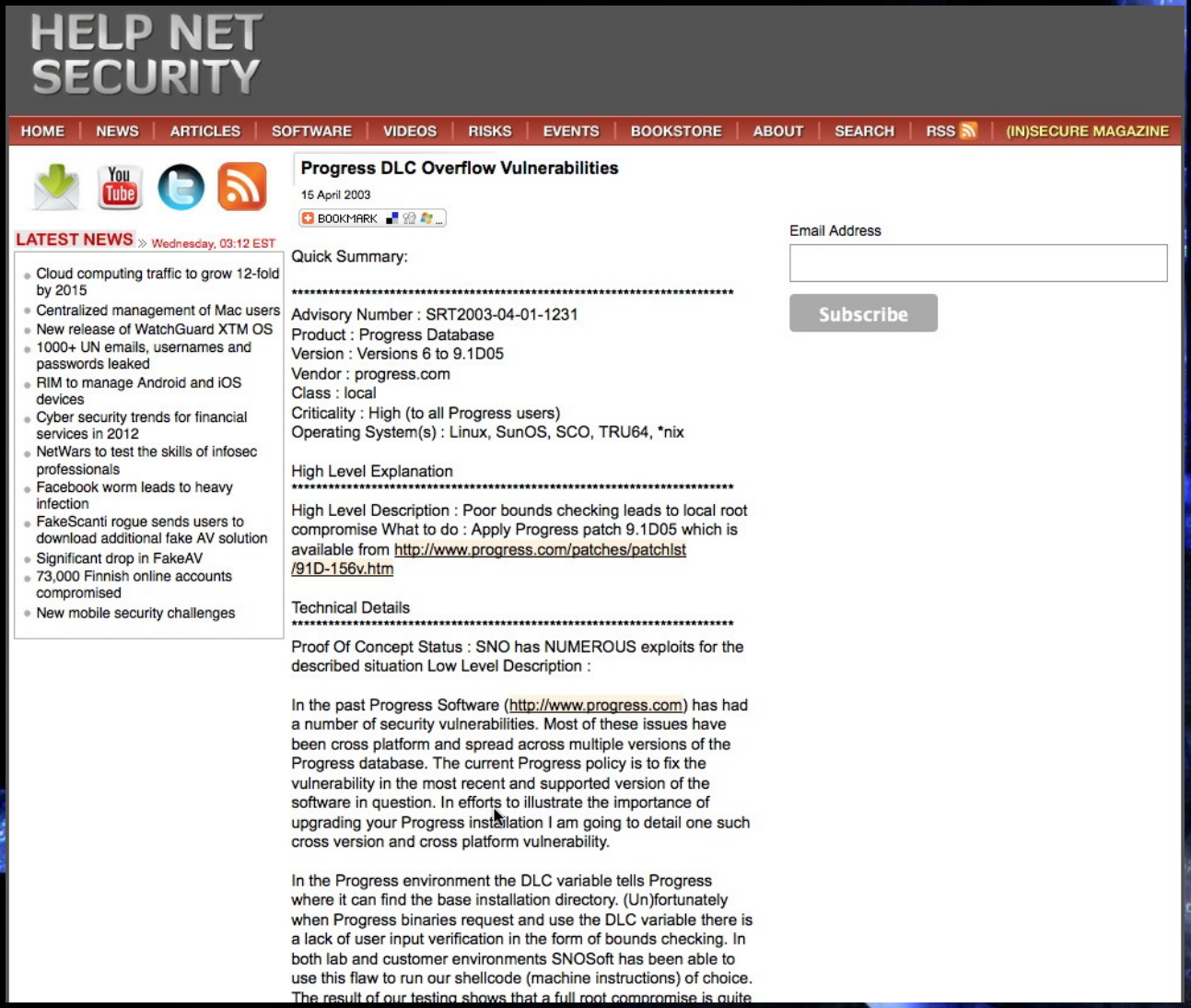
Dealing With Data

- Use the new encryption routines on PID
  - csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
  - Name, Maiden Name, Social Security Number, Credit Card Number, Address, Photo, Fingerprints, etc.

Keep Watch On Warning Orgs

- National Vulnerability Database
  - http://web.nvd.nist.gov/view/vuln/detail?vulnId=
- Net Security Organization
  - http://net-security.org/vuln.php?id=2611
- Progress Software Corporation (keep that maintenance running!)

Keep Watch On Warning Orgs



HELP NET SECURITY

HOME | NEWS | ARTICLES | SOFTWARE | VIDEOS | RISKS | EVENTS | BOOKSTORE | ABOUT | SEARCH | RSS | (IN)SECURE MAGAZINE

LATEST NEWS » Wednesday, 03:12 EST

- Cloud computing traffic to grow 12-fold by 2015
- Centralized management of Mac users
- New release of WatchGuard XTM OS
- 1000+ UN emails, usernames and passwords leaked
- RIM to manage Android and iOS devices
- Cyber security trends for financial services in 2012
- NetWars to test the skills of infosec professionals
- Facebook worm leads to heavy infection
- FakeScanti rogue sends users to download additional fake AV solution
- Significant drop in FakeAV
- 73,000 Finnish online accounts compromised
- New mobile security challenges

Progress DLC Overflow Vulnerabilities

15 April 2003

BOOKMARK

Quick Summary:

****

Advisory Number : SRT2003-04-01-1231
Product : Progress Database
Version : Versions 6 to 9.1D05
Vendor : progress.com
Class : local
Criticality : High (to all Progress users)
Operating System(s) : Linux, SunOS, SCO, TRU64, *nix

High Level Explanation

****

High Level Description : Poor bounds checking leads to local root compromise What to do : Apply Progress patch 9.1D05 which is available from http://www.progress.com/patches/patchlst /91D-156v.htm

Technical Details

****

Proof Of Concept Status : SNO has NUMEROUS exploits for the described situation Low Level Description :

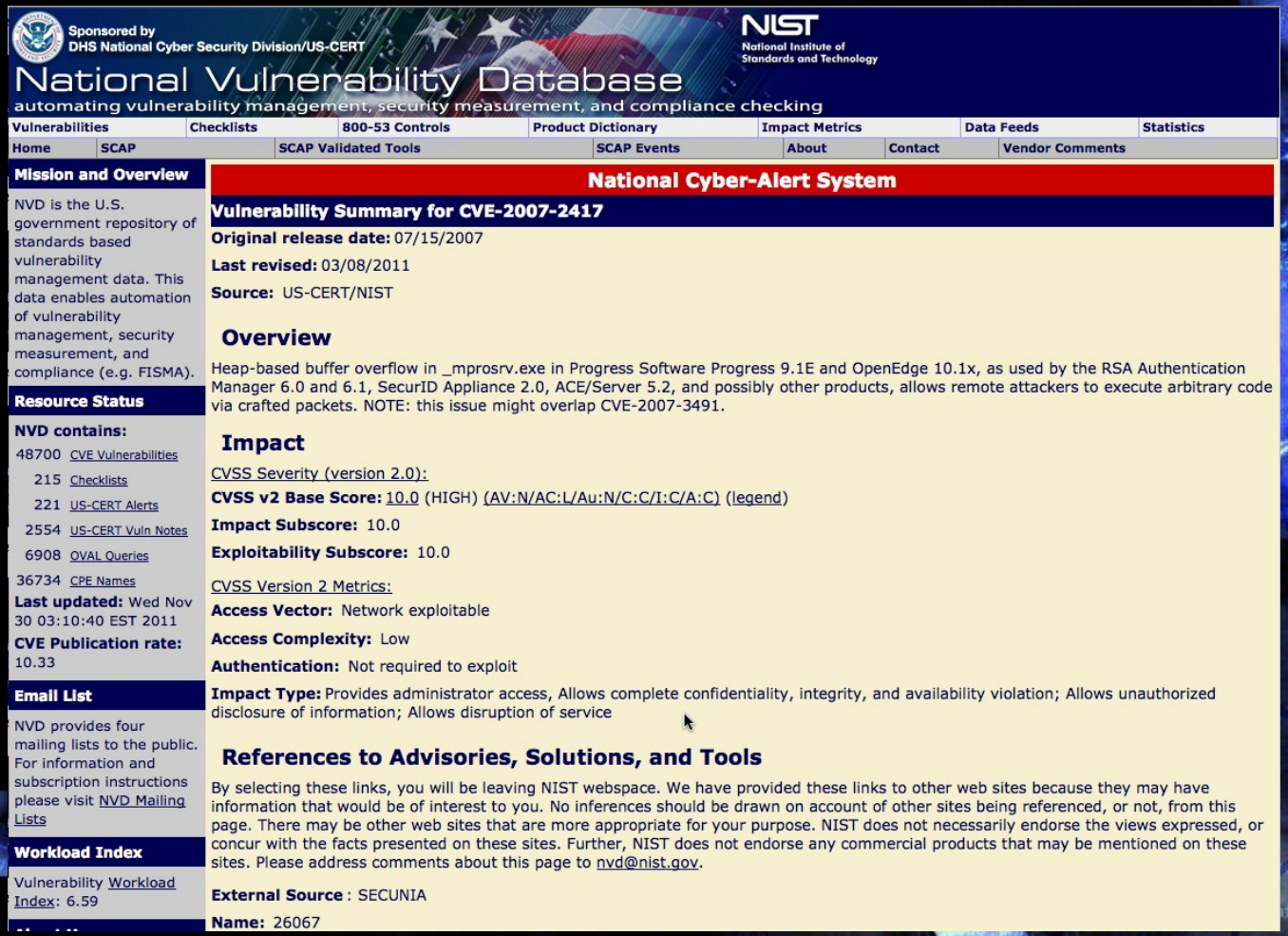
In the past Progress Software (http://www.progress.com) has had a number of security vulnerabilities. Most of these issues have been cross platform and spread across multiple versions of the Progress database. The current Progress policy is to fix the vulnerability in the most recent and supported version of the software in question. In efforts to illustrate the importance of upgrading your Progress installation I am going to detail one such cross version and cross platform vulnerability.

In the Progress environment the DLC variable tells Progress where it can find the base installation directory. (Un)fortunately when Progress binaries request and use the DLC variable there is a lack of user input verification in the form of bounds checking. In both lab and customer environments SNOSoft has been able to use this flaw to run our shellcode (machine instructions) of choice. The result of our testing shows that a full root compromise is quite

Email Address

Subscribe

Keep Watch On Warning Orgs



Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53 Controls | Product Dictionary | Impact Metrics | Data Feeds | Statistics

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

48700 CVE Vulnerabilities
215 Checklists
221 US-CERT Alerts
2554 US-CERT Vuln Notes
6908 OVAL Queries
36734 CPE Names

Last updated: Wed Nov 30 03:10:40 EST 2011

CVE Publication rate: 10.33

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Workload Index

Vulnerability Workload Index: 6.59

National Cyber-Alert System

Vulnerability Summary for CVE-2007-2417

Original release date: 07/15/2007

Last revised: 03/08/2011

Source: US-CERT/NIST

Overview

Heap-based buffer overflow in _mprosrv.exe in Progress Software Progress 9.1E and OpenEdge 10.1x, as used by the RSA Authentication Manager 6.0 and 6.1, SecurID Appliance 2.0, ACE/Server 5.2, and possibly other products, allows remote attackers to execute arbitrary code via crafted packets. NOTE: this issue might overlap CVE-2007-3491.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 10.0 (HIGH) (AV:N/AC:L/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Provides administrator access, Allows complete confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

External Source : SECUNIA

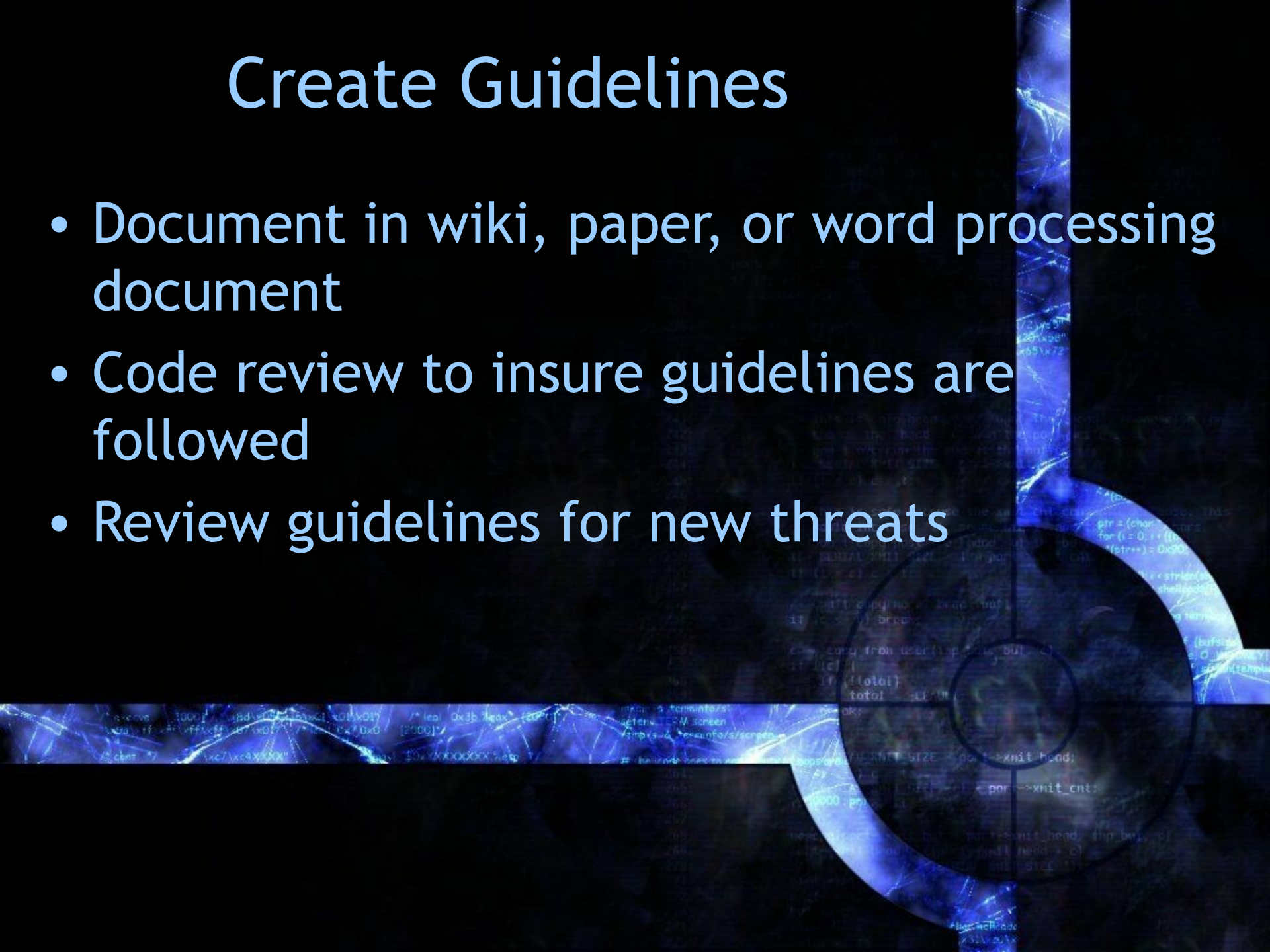
Name: 26067

Legal Consequences

- Torts – Cracker and Database Holder
- Identity Theft
- Security Breach Notification Laws
- A good read:
  - Tort Liability for Lost Personal Computerized Data (South Carolina Law Review)
  - www.stmarytx.edu/law/pdf/Johnsoncyber.pdf

Create Guidelines

- Document in wiki, paper, or word processing document
- Code review to insure guidelines are followed
- Review guidelines for new threats



Questions?

- Email me at sauge@amduus.com
- Planning on making object classes available
- Planning on making documents available
- http://www.linkedin.com/in/scottauge