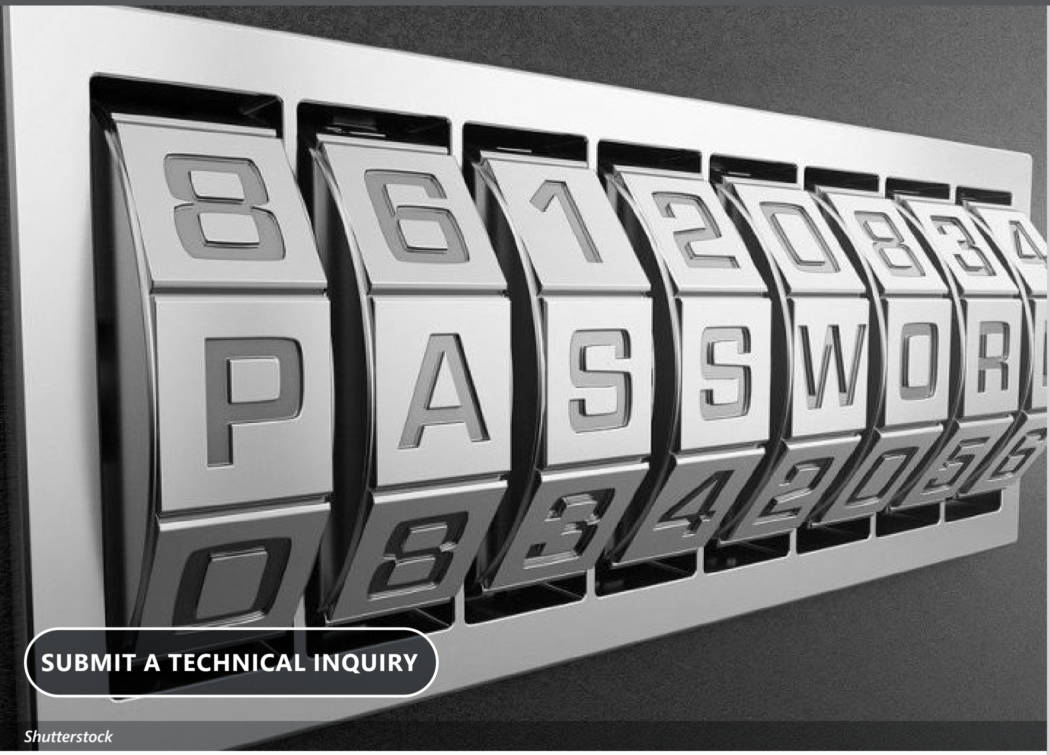
CYBERSECURITY
& Information Systems Digest

The Latest From the Cybersecurity & Information Systems Information Analysis Center // August 31, 2021



SUBMIT A TECHNICAL INQUIRY

Shutterstock

NOTABLE TECHNICAL INQUIRY

How do end-users perceive their own password security practices, and how does this behavior differ from acceptable standards?

Even though technical solutions for security problems are widespread, there are no adequate security measures against precarious user behavior. Even if hashing and encrypting are used correctly in masking the passwords, attackers can bypass these strongpoints by going for the weakest link. Most likely this will happen through sharing a password, using an already leaked password, or creating a feasibly guessable password (Olmstead & Smith, 2017). Furthermore, people seem to feel safe in cyberspace, even if they engage in risky behaviors... **READ MORE**

SNEAK PEEK

UPCOMING WEBINAR
Network Survivability Assessment Methodology

DATE:
September 22, 2021

TIME:
12:00 PM

PRESENTED BY:
Philip Payne

HOST:
CSIAC

VOICE FROM THE COMMUNITY

Keven Hendricks
Detective, Cybercrime Examiner, & Investigator, New Brunswick, NJ, Police Department

Keven Hendricks is a 14-year veteran detective with a municipal police department and has served as a Task Force Officer for two separate federal agencies. He is a published author with the FBI Law Enforcement Bulletin and is currently working as an instructor for Street Cop Training, teaching a class for law enforcement on dark web and cybercrime investigations. He is a Certified Cyber Crime Examiner (3CE) and Certified Cyber Crime Investigator (3CI) by the National White Collar Crime Center (NW3C).

BECOME A SUBJECT MATTER EXPERT

Shutterstock

HIGHLIGHT

AFRL Updates Advanced Computing Tech BAA

On August 5, the U.S. Air Force Research Laboratory (AFRL) posted an updated broad agency announcement (BAA) for Advancing Computing Technology and Applications (BAA NUMBER: FA8750-19-S-7010).

This announcement is for an Open, 2-Step BAA, which is open and effective until 29 September 2024. Only white papers will be accepted as initial submissions; formal proposals will be accepted by invitation only. While white papers will be considered if received prior to 2359 Eastern Standard Time (EST) on 29 September 2024, the agency recommends that submissions for FY23 funding be submitted by 31 May 2022. **LEARN MORE**

FEATURED NEWS

CISA Launches New Joint Cyber Defense Collaborative

The Cybersecurity and Infrastructure Security Agency (CISA) announced the standup of the Joint Cyber Defense Collaborative (JCDC), a new agency effort to lead the development of cyber defense operations plans, and to execute those plans in coordination with partners from the federal interagency, private sector, and state, local, tribal, territorial (SLTT) government stakeholders to drive down risk before an incident and to unify defensive actions should an incident occur.

READ MORE

Image: Shutterstock

LEARN MORE

Shutterstock

WEBINARS

Network Survivability Assessment Methodology

Presented: *September 22, 2021 12:00 PM - 1:00 PM*
Presenter: *Philip Payne*
Host: *CSIAC*

This presentation describes a network survivability assessment methodology for Cyber-Electromagnetic Activities (CEMA) teams to identify cyber threats early in the acquisition cycle.

The DoD Acquisition Process begins with Material Solution Analysis (MSA) and culminates with Operations and Support. An Analysis of Alternatives (AoA) takes place after all potential solutions are examined to fulfill a need and a preliminary acquisition strategy has been established. The AoA consists of an analytical comparison of the operational effectiveness, suitability, and life-cycle cost of materiel solution alternatives that satisfy the established capability need, as described in an Initial Capabilities Document (ICD).

Due to the limited amount of system information that is available during the MSA phase for a set of alternatives being considered, a methodology is required to identify potential system threats early in the acquisition cycle.

According to the AoA Handbook from the Office of Aerospace Studies, effectiveness analysis is normally the most complex element of an AoA. The goal of the effectiveness analysis is to determine the military worth of the alternatives being considered when performing mission tasks (MTs). The network survivability assessment methodology is applied to provide an assessment of existing security controls effectiveness to protect key mission technologies. **LEARN MORE**

EVENTS

Workshop on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software
September 14, 2021

(ISC)^2 2021 Security Congress
October 18, 2021

IEEE Secure Development Conference
October 18, 2021

Cybersecurity Symposium for Smart Cities 2021
October 26, 2021

I/ITSEC 2021
November 29, 2021

DoDIIS Worldwide
December 5, 2021

MORS Emerging Techniques Forum
December 7, 2021

Want your event listed here?
Email contact@csiac.org, to share your event.

Cybersecurity

Knowledge Management
& Information Sharing

Modeling & Simulation

Software Data & Analysis

The inclusion of hyperlinks does not constitute an endorsement by CSIAC or the U.S. Department of Defense (DoD) of the respective sites nor the information, products, or services contained therein. CSIAC is a Defense Technical Information Center (DTIC)-sponsored Information Analysis Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. government or CSIAC.

4695 Millennium Drive Belcamp, MD 21017
443-360-4600 | info@csiac.org | csiac.org
Unsubscribe | Past Digests

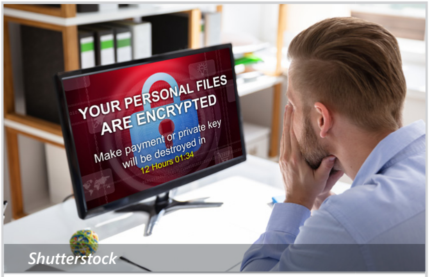
Cybersecurity & Information Systems
Information Analysis Center

RECENT NEWS

iStock

How to Defeat the Info-Warfare "Triad of Disruption"

Cybersecurity and Knowledge Mgmt. & Info. Sharing


YOUR PERSONAL FILES ARE ENCRYPTED
Make payment or private key will be destroyed in
12 Hours 01:34
Shutterstock

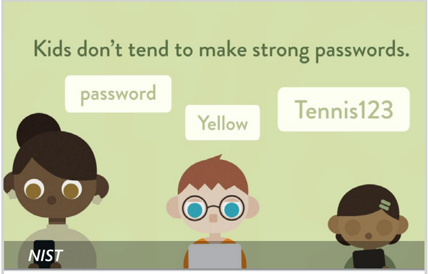
CISA Provides Recommendations for Protecting Information From Ransomware-Caused Data Breaches

Cybersecurity

iStock

Ethical, Legal Implications of Paying Ransoms

Cybersecurity



NIST

NIST Study on Kids' Passwords Shows Gap Between Knowledge of Password Best Practices and Behavior

Cybersecurity

Kubernetes Hardening Guidance

CYBERSECURITY TECHNICAL REPORT

Media Defense

NSA, CISA Release Kubernetes Hardening Guidance

Cybersecurity

NSA

Defeating Malicious Cyber Actors Requires Partnerships

Cybersecurity