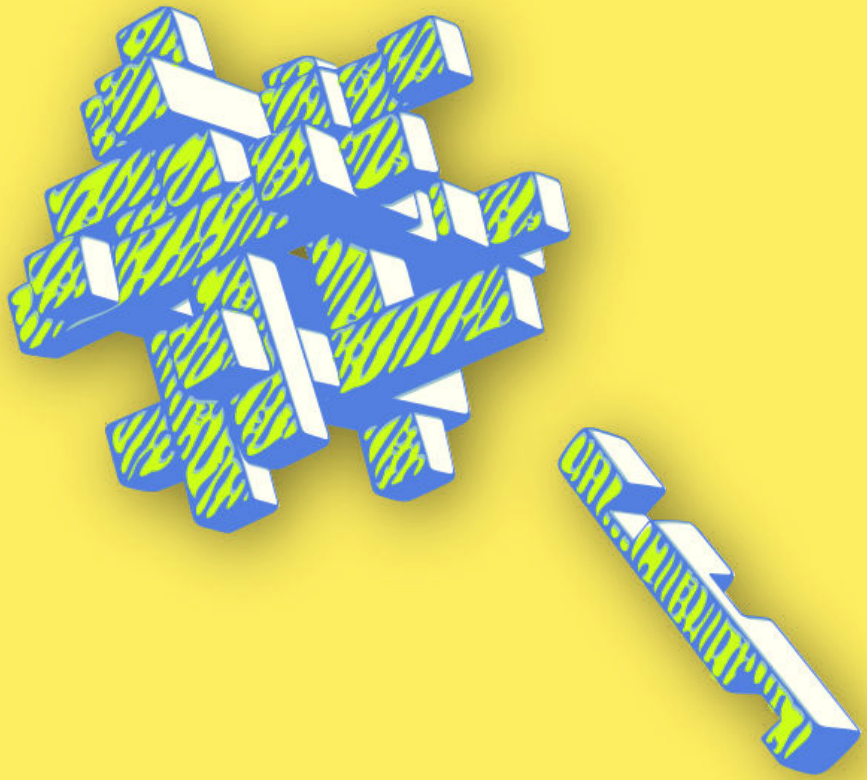

التشفير

التشفير

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

تعريف بمسألة التشفير

- **الأهداف:** هذه الجلسة التعريفية ستشرح للمشاركات مفهوم التشفير، بالإضافة إلى لمحة عامة موجزة عن الأنواع المختلفة للتشفير المتوفر للمستخدمين/ات.
- **الطول:** 50 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** متوسط
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
- **جلسات/تمارين ذات صلة:**
  - الخصوصية[١]
  - الحملات الآمنة على الإنترنت[٢]
  - الإتصالات المشفّرة[٣]
  - التخزين والتشفير[٤]
- **المواد اللازمة:**

[١] https://vrr.im/819e
[٢] https://vrr.im/8e6b
[٣] https://vrr.im/2725
[٤] https://vrr.im/0ccc

- شرائح (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض
- أمثلة عن تقنيات التشفير (مطبوعة)

إدارة الجلسة

الجزء الأوّل – هل سبق لكن أن إستخدمتن التشفير؟

١. إشرحن لهن أن هذه الجلسة جلسة ستعرّفهن على التشفير كمفهوم، لذا لن تتعمّقن كثيرًا في شرح أي من أدوات التشفير التي يحتمل أن تكون المشاركات قد سمعت عنها في السابق (لاسيما جي بي جي GPG/بي جي بي PGP)

٢. قسمن المشاركات إلى مجموعات من شخصين ومن ثمّ إبدأن الجلسة عبر عرض بعض الأمثلة عن تقنيات التشفير. إليكن بعض الأمثلة التي يمكنكن تحضيرها مسبقًا لمشاركتها مع المجموعة:

شيفرة كلمة "بلوبرينتس" BLUEPRINTS

كل حرف من كلمة "BLUEPRINTS" يربط برقم.

S	T	N	I	R	P	E	U	L	B
9	8	7	6	5	4	3	2	1	0

هذا مثال محدد يستعين بكلمة محددة، ولكن يمكن تطبيقه بشكلٍ عام على أي تسلسل أرقام وأحرف – على سبيل المثال، في حال إستخدمتن النظام المذكور أعلاه نفسه، تسلسل الأرقام 82579 يعني كلمة TURNS حين "يُفك التشفير".

يمكنكن أيضًا قلب ترتيب الأرقام بحيث يصبح التسلسل الآن كما يلي

S	T	N	I	R	P	E	U	L	B
0	1	2	3	4	5	6	7	8	9

في هذه الحالة، تسلسل الأرقام 82579 سيدل على تسلسل الأحرف التالي LNPUB (وهذه ليست كلمة) حين "يُفك التشفير"، ولكن مثلا يمكنكن الآن "فكّ تشفير" التسلسل 43206 للتوصل إلى كلمة RINSE.

الرسائل القصيرة القديمة الطراز

إستخدمن صورة للوح مفاتيح هاتف من الطراز القديم (كما يرد أدناه) لعرض نوع آخر من أنواع "التشفير" التي قد تعرفها المشاركات

الرسائل النصية القديمة الطراز

إسألن المشاركات عن كيفية إستخدامهن للوح المفاتيح هذا لكتابة كلمات متنوعة – أحد الأمثلة على ذلك التي يمكنكن الاستعانة بها قد تكون الطلب من كل مشاركة شرح كيفية استخدامها للوح المفاتيح لكتابة اسمها. على سبيل المثال، لكتابة اسم إحدى المشاركات: لينا

Lina، نكتب تسلسل الأرقام التالي 2 66 444 555.

٣. عد أن تنتهين من عرض الأمثلة المذكورة أعلاه، سألن المشاركات إذا ما سبق لهن أن إستخدمن أي نوع من أنواع التشفير – إما نوع شبيه بالأمثلة المذكورة أعلاه وإما أي أمثلة أخرى قد تخطر في بالهن (على سبيل المثال طريقة تشفير شائعة يستخدمها الكثير من الناس في حياتهم اليومية هي "إيتش تي تي بي إس" HTTPS).

٤. إختتمن هذا الجزء من الجلسة عبر طرح سؤال آخر: ما هي العناصر الشائعة التي يمكنهن تحديدها من أمثلة التشفير الأخرى هذه؟

الجزء الثاني – شرح ماهية التشفير

٥. إستنادًا إلى العناصر الشائعة من عناصر التشفير التي حددنها المشاركات في الجزء الأوّل، عليكن الآن التوسّع وشرح المزيد من الأسس والممارسات للمجموعة:

طرق التشفير: خصصن الوقت الكافي لشرح كيفية عمل التشفير إستنادًا إلى الأمثلة من الجزء الأوّل بالإضافة إلى عرض بعض الأمثلة عن صور ملتقطة عن شاشات لشكل البريد الإلكتروني المشفّر بواسطة "جي بي جي". شددن على بعض حالات تنفيذ التشفير الشائعة – وبشكلٍ خاص، خصصن الوقت الكافي لمراجعة تقنية "إيتش تي تي بي إس" والتشفير الكامل وتقنية جي بي جي/بي جي بي.

المفاتيح والمفاتيح الثنائية: إشرحن كيفية عمل مفاتيح التشفير الثنائية والعلاقة الخوارزمية بين المفتاحين العام والخاص. إستعدن الأمثلة عن التطبيقات المذكورة آنفًا (إيتش تي تي بي إس، التشفير الكامل وجي بي جي/بي جي بي) وإشرحن أنه لكل واحدة من هذه التطبيقات مفاتيح خاصة مخزّنة و/أوظاهرة للمستخدم.

ممارسات التشفير: ألقين الضوء على أهم الممارسات الفضلى المرتبطة بالتطبيقات الشائعة للتشفير، كتقنية التحقق من البصمة والتوقيع الرقمي على المفاتيح لعرض ذلك، أطلبن من المشاركات تحديد المكان في تطبيق سيجنال الذي يمكن للمستخدم فيه التحقق من

بصمة مستخدم آخر، وعلى نحو مماثل، في حال كانت المشاركات تمتلكن مفاتيح جي بي جي/بي جي بي، يمكنكن مناقشة فوائد ومساوئ توقيع وتوزيع المفاتيح المتاحة للعموم. والوقت مناسب أيضًا لمناقشة المراسلات المشفرة تشفيرًا كاملاً في تطبيقات المحادثة كتطبيق سيجنال وواتساب وتليغرام- ذكّرن المشاركات أن التشفير الكامل ليس دائمًا مفعّلًا بشكلٍ تلقائي على بعض هذه الخدمات.

النسخ الإحتياطية المشفّرة: إستنادًا إلى مثال التشفير بواسطة جي بي جي/بي جي بي المذكور أعلاه، إسألن المشاركات إذا كنّ يعتقدن أن القيام بنسخة إحتياطية لمفتاح جي بي جي الخاص بهن فكرة جيّدة، وإن كان كذلك، ما هي الخطوات التي يمكنهن إتباعها؟

المراجع

- https://www.gnupg.org/gph/en/manual/book1.html

باب ٢

الإتصالات المشفّرة

- **الأهداف:** تستند هذه الجلسة إلى محتويات التدريب السابقة المرتبطة بالتشفير، ناقلةً إلى المشاركات أهمية تشفير الإتصالات وفائدتها وتقديم الأدوات المهمة لذلك
- **الطول:** 50 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** متوسط
- **المعرفة المطلوبة:**
  - معرفة مفاهيم الأمن الرقمي الأساسية و/أوتدريب مسبق
  - تعريف بمسألة التشفير (التشفير)
- **جلسات/تمارين ذات صلة:**
  - الخصوصية[١]
  - الحملات الآمنة على الإنترنت[٢]
  - تعريف بمسألة التشفير[٣]
- **المواد اللازمة:**

[١] https://vrr.im/819e
[٢] https://vrr.im/8e6b
[٣] https://vrr.im/f5d4

- شرائح (فيها النقاط المفتاحية الواردة أدناه)
- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز عرض

إدارة الجلسة

١. إبدأن الجلسة بمشاركة بعض الأمثلة المهمة عن حالات يكون فيها تشفير الإتصالات مفيدًا، وخصصن الوقت اللازم لشرح كيفية عمل التشفير. أعرضن بواسطة بعض أمثلة عن صور لشاشات بريدًا إلكترونيًا مشفّرًا بواسطة جي بي جي لإظهار كيف تبدو الرسائل ورسائل البريد الإلكتروني حين تكون مشفّرة وسلطن الضوء على التطبيقات الشائعة للتشفير – لا سيما تقنية إيتش بي بي إس والتشفير الكامل وتشفير جي بي جي/بي جي بي.

٢. إحصرن النقاش الآن بالتحديد على الأدوات التي تسمح بتشفير الإتصالات: تطبيق سيجنال للإتصالات والرسائل، وتطبيق "ميت.جيتسي" https://meet.jitsi لاتصالات الفيديو وتوتانوتا أو جي بي جي و"ثندر بيرد" Thunderbird لرسائل البريد الإلكتروني. كلها أمثلة مفيدة لابد من مشاركتها.

٣. إشرحن الفوائد الأمنية لهذه الأدوات للمجموعة، وبشكلٍ أساسي كيف تمكّن المستخدمين من الحد من إمكانية وصول الآخرين إلى اتصالاتهن؛ ومن ثمّ ناقشن الحالات التي قد يتعرض فيها أمن بيانات المستخدم لخطر الإنكشاف، حتى مع إستخدام الإتصالات المشفّرة. إسألن المشاركات – كيف يمكن أن تتعرض محتويات بريد إلكتروني مشفّر بواسطة جي بي جي لخطر الإنكشاف بسبب تسجيل المفاتيح (keylogging) أوبرمجيات الخبيثة لإلتقاط صور الشاشة (screen-apturing malware) ؟ ما الذي قد يحدث في حال تمكن أحد الخصوم من الوصول إلى مفتاح جي بي جي خاص بمستخدم/ة – كيف يمكن للخصوم استخدامه للوصول إلى بياناتهن؟

٤. في حال كان الوقت المتوفر يسمح بذلك، لابد من توفير فرصة الممارسة التطبيقية للمشاركات على الأقلّ على واحدة من الأدوات المذكورة آنفًا في المرحلة الثانية. ومع

أن الوقت قد لا يكون متاحًا لتعليم المجموعة كيفية إعداد تقنية جي بي جي/بي جي بي للبريد الإلكتروني، يمكنكن اختيار عرض إتصال فيديو محمي بتقنية إيتش تي تي بي إس عبر تطبيق "ميت.جيتسي"، أوأطلبن من المشاركات تثبيت تطبيق سيجنال على هواتفهن للتدرّب على إرسال الرسائل المشفّرة إلى بعضهن البعض، أوتبادل الاتصالات الهاتفية المشفّرة.

المراجع

- https://ssd.eff.org/en/module/how-use-signal-android
- https://ssd.eff.org/en/module/how-use-signal-ios